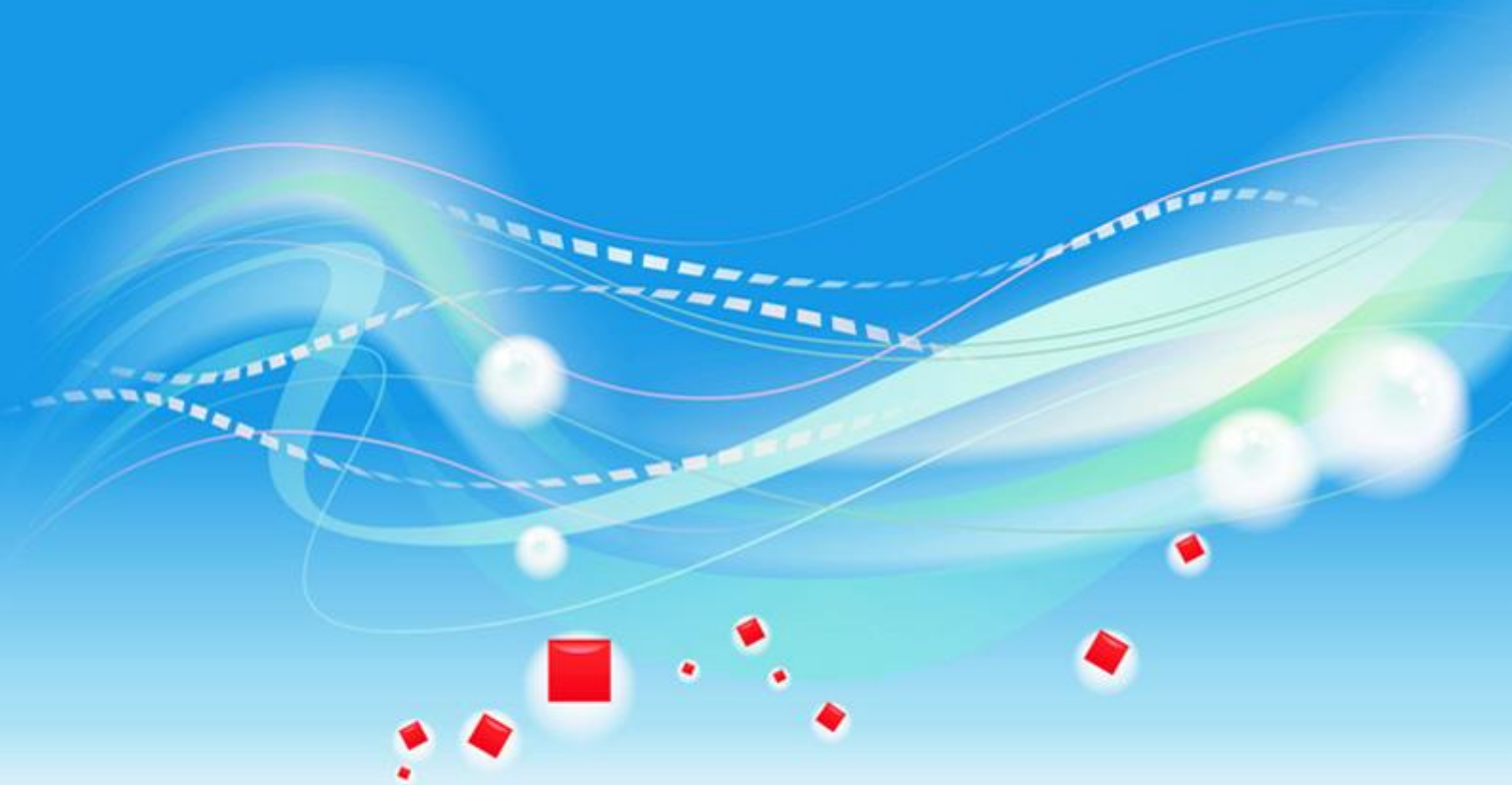

ViPNet StateWatcher: Monitoring System for ViPNet Networks. Monitoring Web Access

User's Guide

ViPNet Virtual Private Network

infotecs

© 1991–2014 Infotecs. All rights reserved.

Version: 00056-08 34 01 ENU

This document is included in the software distribution kit and is subject to the same terms and conditions as the software itself.

No part of this publication may be reproduced, published, stored in an electronic database, or transmitted, in any form or by any means — electronic, mechanical, recording, or otherwise — for any purpose, without the prior written consent of Infotecs JSC.

ViPNet® is a registered trademark of Infotecs JSC, Moscow, Russia.

All brands and product names that are trademarks or registered trademarks are the property of their owners.

Global contacts page http://www.vipnet.com/index_all.php

Contents

Introduction **6**
About This Document 7
Audience 7
Document Conventions 7
About Monitoring Web Access 9
Distribution Kit 9
System Requirements 10
What's New in Version 4.3 13
Feedback 17

Chapter 1. General Information **18**
Recommended Internet Explorer Configuration 19
Starting and Ending a Monitoring Session 22
Changing a User Password 25
Interface of the Host List Page 26

Chapter 2. ViPNet Host Monitoring **28**
Monitoring Hosts in the Host List 29
Viewing the Monitored Hosts List 29
Monitored Hosts List 29
Host Groups 31
Viewing Information about a Monitored Host 32
Viewing Information about the Events Registered on Hosts 35
Polling Monitored Hosts 35
Filtering Monitored Hosts 36
Monitoring Hosts on a Dashboard 38
Configuring Dashboard 39
Configuring a Current Settings Tile 41
Configuring a Graph Tile 42
Monitoring Hosts on a Map 45
Recentering the Map and Positioning on the Map 47
Searching for Hosts on the Map 48

Searching for Geographical Objects 49
Viewing Information about a Monitored Host 50
Viewing Information about a Monitored Hosts Group 50
Viewing the Monitoring Events History 52
Detailed Viewing of the Monitoring Events History 54
Exporting the Monitoring Events History 55
Exporting Unprocessed Host Parameters 57
Working with Notifications 60
Visual notifications in the Host List 60
Pop-up Messages 61
Configuring Pop-up Notifications 63
Visual notification on the Map 64
Sound Notifications 64
Email Notifications 65
ViPNet Business Mail Notifications 65
SMS Notifications 66
Statistics 67
Viewing the Statistics for a Cascade Segment 68
Monitoring the Network Health 71

Appendix A. Troubleshooting 73
Can't Connect to the Monitoring Server via a Web Browser 73
Possible Malfunctions 74
Too Many Monitored Hosts. 75
Monitoring Server is Unavailable 75
StateWatcher Role Is Not Registered 76
Cannot Open a Host Details Window 76
Need to Re-Authenticate the User 77
Problems During Unprocessed Host Parameters Exporting 77

Appendix B. Structure of the Unprocessed Host Parameters Export File 78

Appendix C. Structure of the Events History Export File 86

Appendix D. Monitored Parameters 88
Parameters Monitored on Hosts 89
Parameters Monitored on Public Hosts 103

ViPNet IDS Monitoring Parameters..... 116

Appendix E. Glossary 121

Appendix F. Index..... 127

Introduction

About This Document 7

About Monitoring Web Access 9

What's New in Version 4.3 13

Feedback 17

About This Document

This document describes the purpose and scope of Monitoring Web Access that is a part of the ViPNet StateWatcher monitoring system. It contains information on the basic features and operating principle of the interface. Also, the document describes the user interface of this program.

This document presents guidelines on how to view data and statistics gathered from monitored hosts (see Monitored host on page 122), to export options of the monitored hosts and the monitoring events history. Also, it describes the work with notifications.

This document is a part of the documentation kit distributed with ViPNet StateWatcher monitoring system. The documentation kit consists of the following documents:

- ViPNet StateWatcher: Monitoring System for ViPNet Networks. Overview.
- ViPNet StateWatcher: Monitoring System for ViPNet Networks. Monitoring Server. Administrator's Guide.
- ViPNet StateWatcher: Monitoring System for ViPNet Networks. Monitoring Web Access. User's Guide (this document).

Audience

This document is intended for ViPNet StateWatcher users who monitor ViPNet hosts via Monitoring Web Access.

It is also intended for ViPNet StateWatcher administrators who can perform all user scenarios plus a number of specific ones. The administrator-only scenarios are described in a special document: "ViPNet StateWatcher: Monitoring System for ViPNet Networks. Monitoring Server. Administrator's Guide."

Document Conventions

This document concerns the following conventions:

Table 1: Document conventions

Icon	Description
	Warning: Indicates an obligatory action or information which may be critical for continuing user operations.
	Note: Indicates a non-obligatory, but desirable action or information which may be helpful for users.
	Tip: Contains additional information.

Table 2: Conventions for highlighted information

Icon	Description
Name	The name of an interface element. For instance, the name of a window, a box, a button or a key.
Key+Key	Shortcut keys. To use the shortcut keys, press and hold the first key and press other keys.
Menu > Submenu > Command	A hierarchical sequence of elements. For instance, menu items or sections in the navigation pane.
`Code`	A file name, path, text file (code) fragment or a command executed from the command line.

About Monitoring Web Access

Monitoring Web Access (MWA) is a part of the ViPNet StateWatcher monitoring system.

You can connect to this web application from a Windows OS computer with the ViPNet Client software and a web browser installed.

MWA provides remote access to the Monitoring Server program and to its database. In MWA, users can view data about monitored hosts' status, the statistics which is collected from hosts, monitoring events history, and more.

The Monitoring Server administrators can not only view data in the Monitoring Server database, but also change settings of the Monitoring Server program.

For more information about the Monitoring Server settings, see the document "ViPNet StateWatcher: Monitoring System for ViPNet Networks. Monitoring Server. Administrator's Guide," which is included in the ViPNet StateWatcher distribution kit.

Distribution Kit

All the components distributed with Monitoring Web Access are specified in the table below.

Table 3: Distribution kit

	Item	File name
Software required for monitoring via Monitoring Web Access	Adobe Flash Player plug-in for Mozilla Firefox browser	`flashplayer_11_plugin_debug_32bit.exe`
	Adobe Flash Player plug-in for Internet Explorer browser	`flashplayer_11_ax_debug_32bit.exe`
	There is Adobe Flash Player plug-in in Google Chrome browser,	therefore it is not included in the distribution kit.
	You can download a setup file for the iReport visual designer from http://jasperforge.org/projects/ireport/ http://jasperforge.org/projects/ireport/	`iReport-3.7.6-windows-installer.exe`
Documentation in PDF	ViPNet StateWatcher: Monitoring System for ViPNet Networks. Overview	`vipnet_statewatcher.pdf`

ViPNet StateWatcher: Monitoring System for ViPNet Networks. Monitoring Web Access. User's Guide	`vipnet_statewatcher_userguide.pdf`
ViPNet StateWatcher: Monitoring System for ViPNet Networks. Monitoring Server. Administrator's Guide	`vipnet_statewatcher_admguide.pdf`

System Requirements

You can work in Monitoring Web Access on any ViPNet host where the ViPNet Client software (any version) is installed.

Warning: For the correct work of Monitoring Web Access, you need to accept and install the latest Windows OS updates.

The minimum system requirements for your computer to run Monitoring Web Access are as follows:

- Processor: Intel Pentium IV or any other x86-compatible processor of similar characteristics.
- Minimum RAM: 512 MB (1 GB recommended).
- Operating system: Microsoft Windows XP SP3 (32-bit), Server 2003 (32-bit), Vista SP2 (32/64-bit), Server 2008 (32/64-bit), Windows 7 (32/64-bit), Server 2008 R2 (64-bit), Server 2012 (64-bit), Server 2012 R2 (64-bit), and Windows 8 (32/64-bit).
- Access to the Internet if you want to send SMS notifications.

For your Monitoring Web Access to work efficiently (for example, when you need to monitor many hosts or for better detailization on maps), we recommend you to use a more powerful computer:

- Processor: Intel Core 2 Quad or any other x86-compatible processor of similar characteristics.
- Minimum RAM: 8 GB.

- Operating system: Microsoft Windows Vista SP2 (64-bit), Server 2008 (64-bit), Windows 7 (64-bit), Server 2008 R2 (64-bit), Server 2012 (64-bit), Server 2012 R2 (64-bit), and Windows 8 (32/64-bit).
- Access to the Internet if you want to send SMS notifications.

We recommend you to use the screen resolutions listed below.

Table 4: Recommended screen resolutions for Monitoring Web Access

Recommended resolutions	Partially supported resolutions
1400 x 1050	1024 x 768
1600 x 1200	1280 x 768
1680 x 1050	1280 x 800
1920 x 1080	1280 x 1024
	1360 x 768
	1440 x 900
	1600 x 900

Note: If you use partially supported screen resolutions, some web pages may exceed your screen bounds.

For viewing web pages without scroll bars, set the screen resolution to 1280 x 1024 or higher.

We don't recommend you to use screen resolution 1280 x 600 when you work in Monitoring Web Access.

One of the following browsers should be installed:

- Microsoft Internet Explorer (versions from 8.0 to 11);
- Firefox (versions from 4.0 to 32.0). You can download the latest version from www.mozilla.org/en-US/firefox/new/ www.mozilla.org/en-US/firefox/new/;
- Google Chrome (versions from 11.0 to 37.0).

Tip: We recommend you to use the latest browser versions.

We don't recommend you to open Monitoring Web Access in different browsers or different windows/tabs of the same browser simultaneously. Also, we don't recommend you to work in Monitoring Web Access using more than one account at a time.

Warning: For Monitoring Web Access to work correctly, enable JavaScript and Cookies in your browser. For more information about enabling and disabling these features, see Help to your browser.

If you use Internet Explorer version 9.0, disable the high security level in the Internet Options (see Recommended Internet Explorer Configuration on page 19).

For sound notifications, the Adobe Flash Player plug-in is required. The plug-in is downloaded automatically by your browser when there is an Internet connection. Otherwise, you can download it from http://get.adobe.com/flashplayer/.

What's New in Version 4.3

This section contains a brief description of changes made to the ViPNet StateWatcher monitoring system and its new features in version 4.3 in comparison to version 4.2.1. You can find information about earlier versions of the monitoring system in the document "ViPNet StateWatcher: Monitoring System for ViPNet Networks. Overview" in the appendix Version History.

- **Monitoring hosts on the dashboard**

  You can configure the dashboard to acquire up-to-date information about monitored hosts in a handy form. You can choose parameters for display on the **Dashboard** page. On the dashboard, current values of monitored hosts' parameters can be displayed in graphs or on a map (see Monitoring Hosts on a Dashboard on page 38).

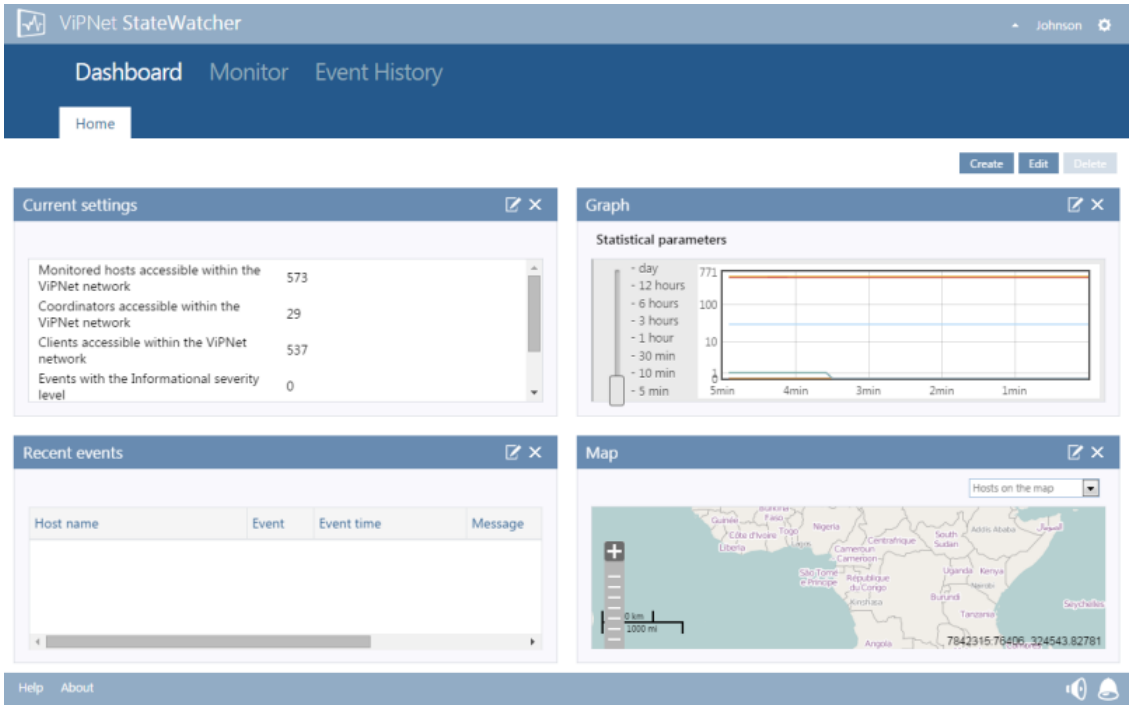

Figure 1: Dashboard

- **Adding a host description**

  In the **Host Information** window, the **Description** tab has been added for MWA users to type any useful information about the host (see Viewing Information about a Monitored Host on page 32). The added information can be viewed and edited by other users.

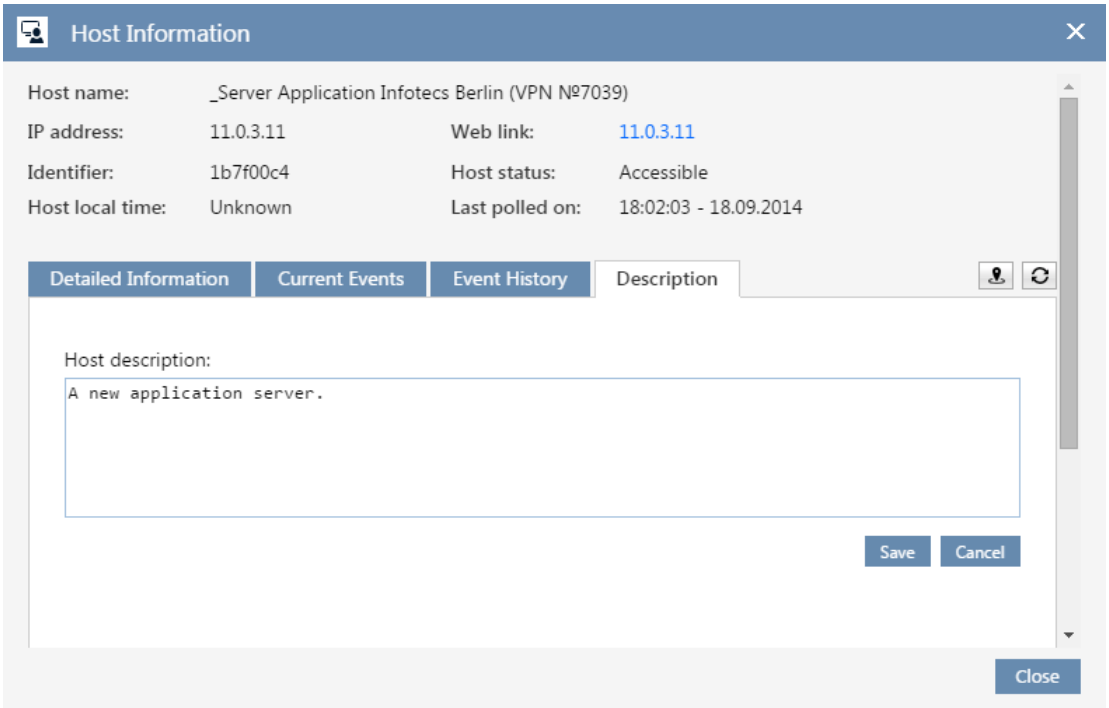

Figure 2: Adding host description

- **Monitoring connection to coordinators**

  You can monitor connection between the selected host and ViPNet coordinators with which it is linked. For your convenience all coordinators are displayed on one list in the monitored host properties window. Thus, you can quickly find out which network segment is disconnected. Moreover, you can configure the display of these data on the dashboard.

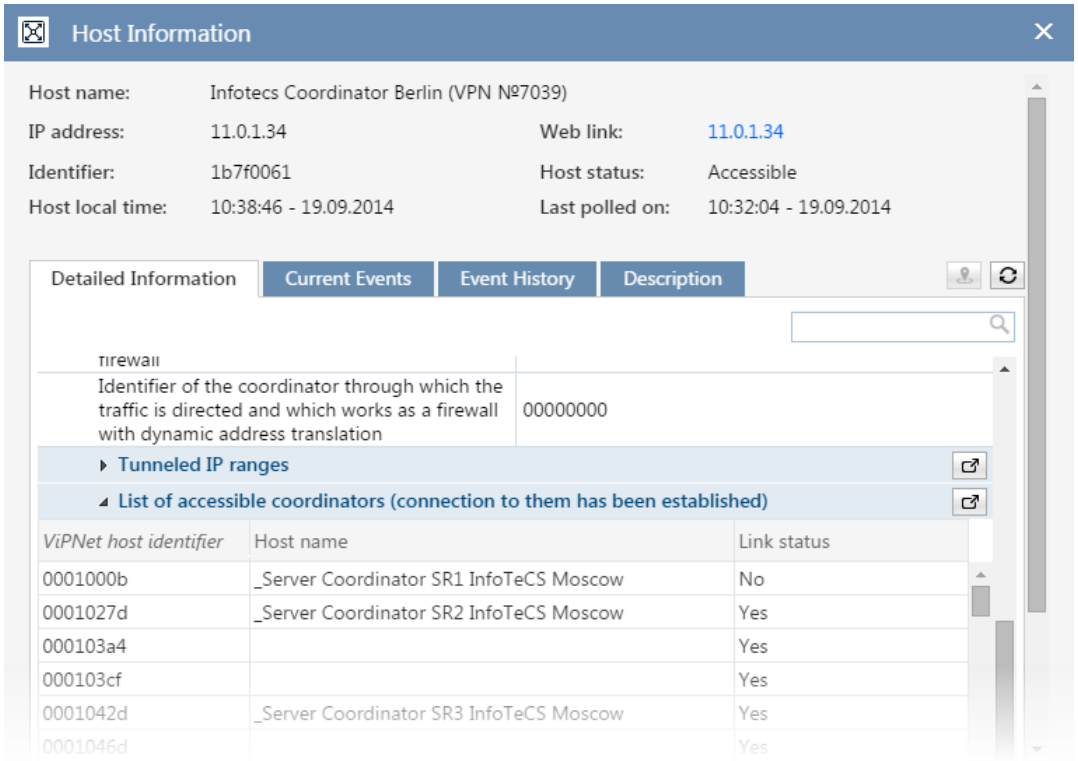

Figure 3: Viewing the connection status of a host with ViPNet coordinators

- **Changes to Monitoring Web Access Interface**

  The monitoring web interface has been improved and updated. Flat UI design has been developed for MWA, fonts are easier to read, and icons have been redesigned.

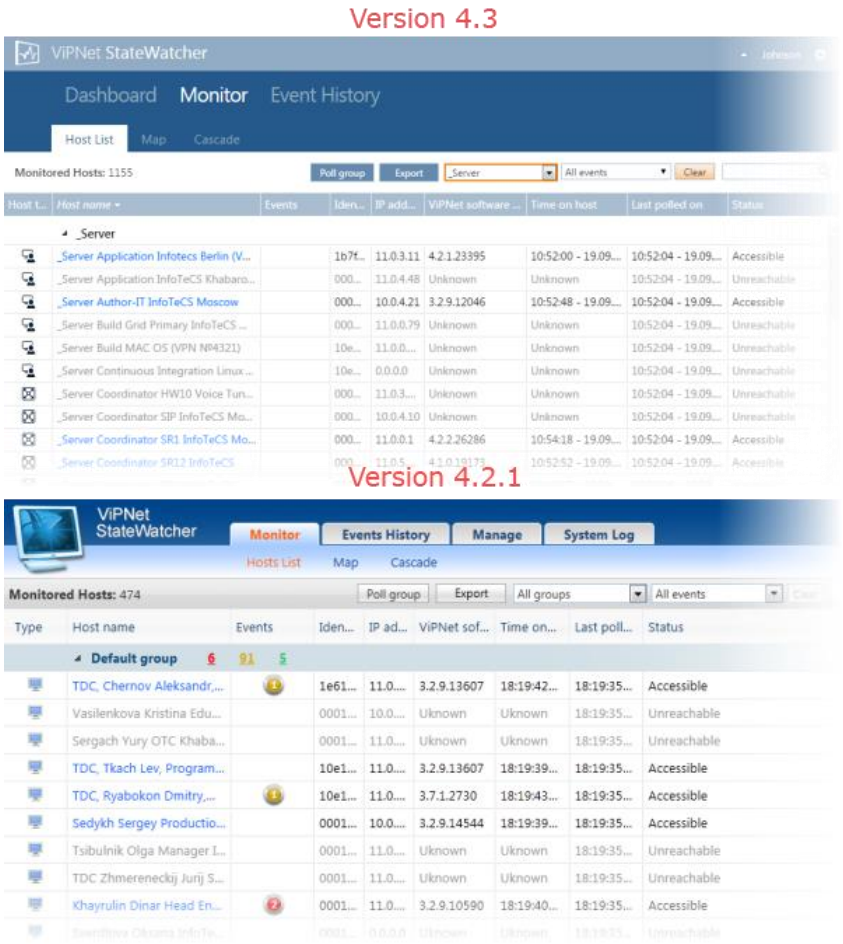

Figure 4: Interface differences

Feedback

Finding Additional Information

For more information about Infotecs products and technologies, see the following resources:

- ViPNet documentation web portal http://www.vipnet.com/redir/doc_vipnet/.
- Information about current Infotecs products http://www.infotecs.ru/solutions/.
- Information about Infotecs solutions http://www.vipnet.com/redir/solutions/.

Contacting Infotecs

We value any feedback from you. If you have any questions concerning Infotecs products and solutions, any suggestions, complains or other feedback, feel free to contact us by means of the following:

- Global contacts page http://www.vipnet.com/index_all.php
- Telephone (Germany): +49 (0) 30 206 43 66 0
- Telephone (USA): +1 (646) 589-8571

Errata

Infotecs makes every effort to ensure that there are no errors or misprints in the text of all documents supplied with ViPNet software. However, no one is perfect, and mistakes do occur. If you find an error in one of our documents, like a spelling mistake or some inaccuracy in describing user scenarios or system features, we would be very grateful for your feedback. By sending in errata you may save other reader hours of frustration, and at the same time you will be helping us provide documentation of even higher quality.

1

General Information

Recommended Internet Explorer Configuration 19

Starting and Ending a Monitoring Session 22

Changing a User Password 25

Interface of the Host List Page 26

Recommended Internet Explorer Configuration

In order to correctly display the web interface, Internet Explorer should not be in Compatibility View mode.

If you use Internet Explorer 8, prior to starting the Monitoring Web Access make sure that the required parameters are set in Internet Options. To do this:

1. Run Internet Explorer.
2. On the **Tools** menu, click **Internet Options**.
3. On the **Advanced** tab, under **Multimedia**, select the **Play animations in webpages** and **Play sounds in webpages** check boxes.

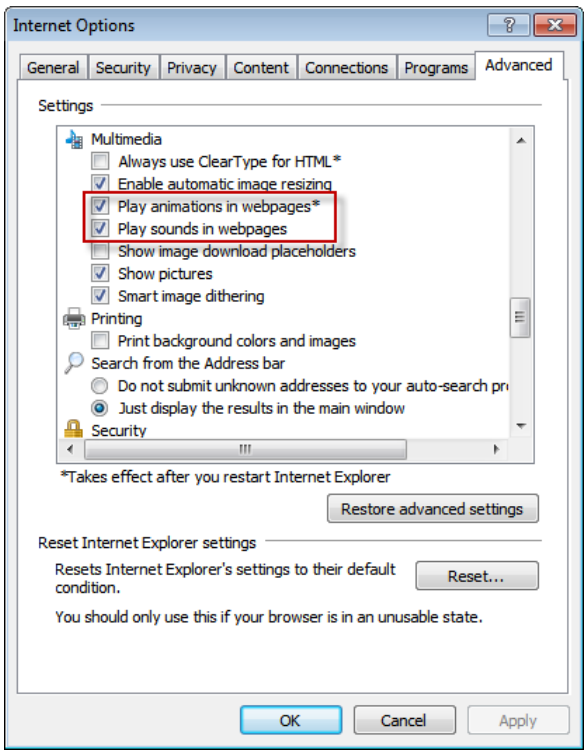

Figure 5: Advanced Internet Explorer configuration

4. In the **Internet Options** dialog box, click **Apply**.

If you are using the Internet Explorer 9 web browser and Windows Server 2003 or Windows Server 2008 R2, you should disable Enhanced Security Configuration. For this, depending on the used OS, do the following:

1 For Windows Server 2003:

1.1 Click the **Start** button and then click **Control Panel** > **Add or Remove Programs**.

1.1 In the displayed window, click **Add or remove Windows components**. The **Windows Components Wizard** will be started.

1.2 On the first page, in the **Components** list, clear the **Internet Explorer Enhanced Security Configuration** check box and click **Next**.

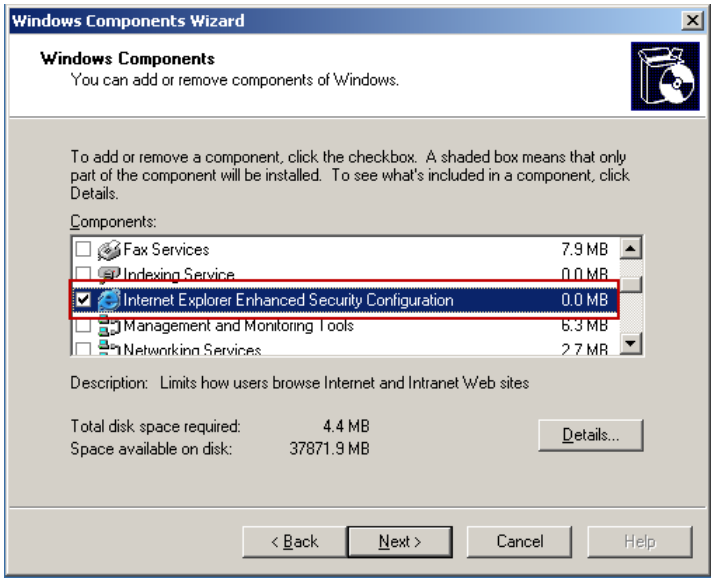
Windows Components Wizard
Windows Components
You can add or remove components of Windows.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Fax Services 7.9 MB
Indexing Service 0.0 MB
Internet Explorer Enhanced Security Configuration 0.0 MB
Management and Monitoring Tools 6.3 MB
Networking Services 2.7 MB
Description: Limits how users browse Internet and Intranet Web sites
Total disk space required: 4.4 MB
Space available on disk: 37871.9 MB
Details...
< Back
Next >
Cancel
Help

Figure 6: Disabling Enhanced Security Configuration for Windows Server 2003

1.3 To exit the wizard, click **Finish**.

2 For Windows Server 2008 R2:

2.1 Click the **Start** button, and then click **Control Panel**.

2.2 In the **All Control Panel Items** window, click **Programs and Features**.

2.3 In the **Programs and Features** window, click **Turn Windows features on or off**.

2.4 In the **Server Manager** window, under **Server Summary** > **Security Information**, click **Configure IE ESC**.

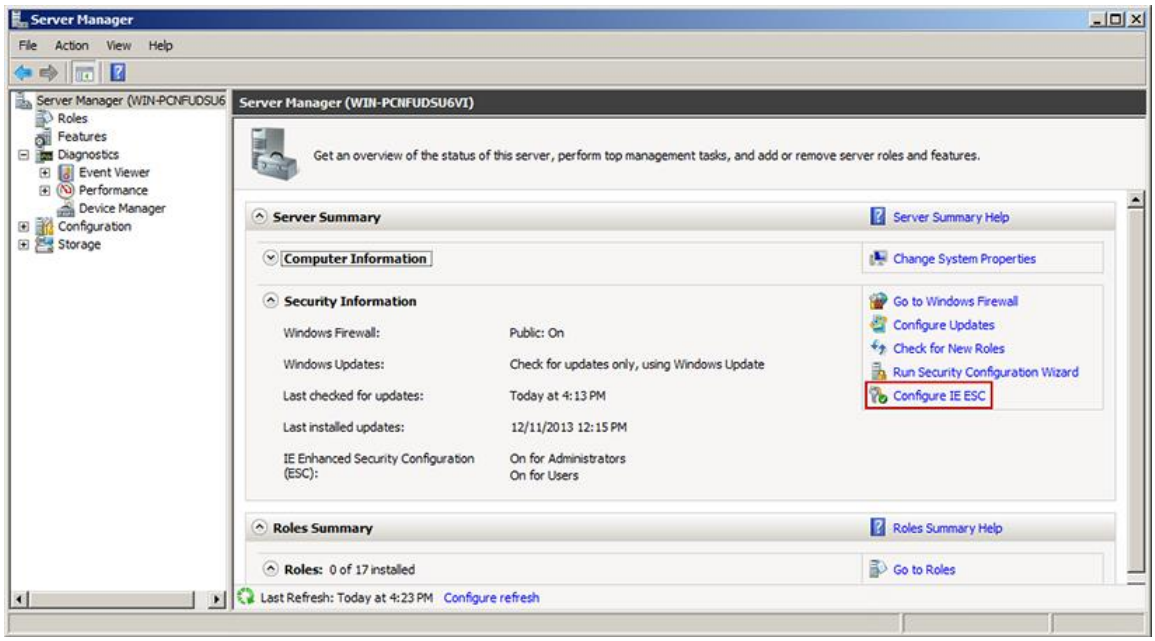
Server Manager
File Action View Help
Server Manager (WIN-PCNFUDSU6
Roles
Features
Diagnostics
Event Viewer
Performance
Device Manager
Configuration
Storage
Server Manager (WIN-PCNFUDSU6VI)
Get an overview of the status of this server, perform top management tasks, and add or remove server roles and features.
Server Summary
Server Summary Help
Computer Information
Change System Properties
Security Information
Go to Windows Firewall
Configure Updates
Check for New Roles
Run Security Configuration Wizard
Configure IE ESC
Windows Firewall: Public: On
Windows Updates: Check for updates only, using Windows Update
Last checked for updates: Today at 4:13 PM
Last installed updates: 12/11/2013 12:15 PM
IE Enhanced Security Configuration (ESC): On for Administrators On for Users
Roles Summary
Roles Summary Help
Roles: 0 of 17 installed
Go to Roles
Last Refresh: Today at 4:23 PM Configure refresh

Figure 7: Setting Enhanced Security Configuration in Internet Explorer

2.5 In the displayed window, for **Administrators** and **Users**, select **Disable** and click **OK**.

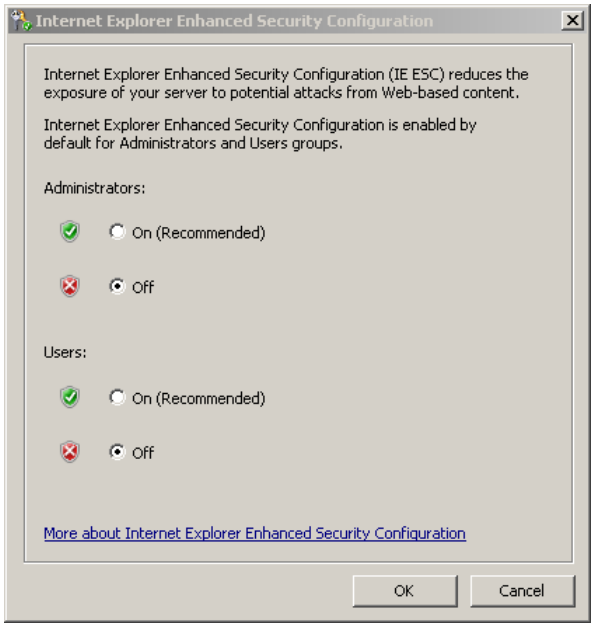
Internet Explorer Enhanced Security Configuration
Internet Explorer Enhanced Security Configuration (IE ESC) reduces the exposure of your server to potential attacks from Web-based content.
Internet Explorer Enhanced Security Configuration is enabled by default for Administrators and Users groups.
Administrators:
On (Recommended)
Off
Users:
On (Recommended)
Off
More about Internet Explorer Enhanced Security Configuration
OK
Cancel

Figure 8: Disabling Enhanced Security Configuration in Internet Explorer

Starting and Ending a Monitoring Session

To start working in Monitoring Web Access:

1. Connect to the monitoring server. There are two ways to do this:
   - Open a web browser and in the address bar type `http://<monitoring_server_address>:<port_number>`. Specify the IP address of the monitoring server you want to connect to. A port number should be typed only if it is not the default one (the default port number is 80). You may ask your ViPNet administrator about your monitoring server address and the port number.
   - In the ViPNet Monitor program, in the **Private Network** section, click your monitoring server and do one of the following: on the toolbar, click **Web**; on the **Actions** menu or on the context menu, click **Open Web Resource on this ViPNet Host**.

   After you connect to the monitoring server successfully, the logon window will be displayed.

Figure 9: User logon

2 In the **User** box, type the account name, and in the **Password** box, type the password to this account and click **Log in**. User name, password, and other user attributes are specified by the Monitoring Server administrator when he or she creates a user account.

After logon, a page with a list of monitored hosts will be displayed.

Note: The first time you connect to Monitoring Server, you might come across a problem that there are no monitored hosts on the list and on other pages. This may occur if the StateWatcher administrator has not specified any monitored hosts. In this case, ask your administrator to do this.

To finish your monitoring session, on any page, under your account name, click the **Log off** link. Your browser will continue working and the logon window will be displayed.

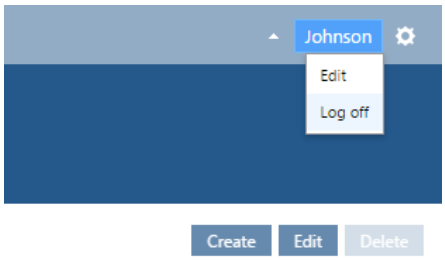

Figure 10: Logging off from the monitoring system

Changing a User Password

You may change your password at any time. To change the password:

1. In the upper right corner of the web page, on the menu with your user name, click **Edit**. The password change window will be displayed. In the **Name** box, your user name will be displayed.

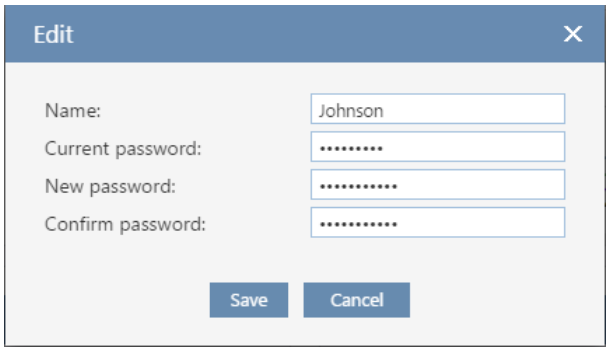

Figure 11: Changing a user password

2. In the corresponding box, type the current password. Then, in the **Confirm password** box, type the new password and confirm it.

3. To change the password, click **Save**. To discard changes, click **Cancel**.

Interface of the Host List Page

The **Host list** page is shown in the figure below:

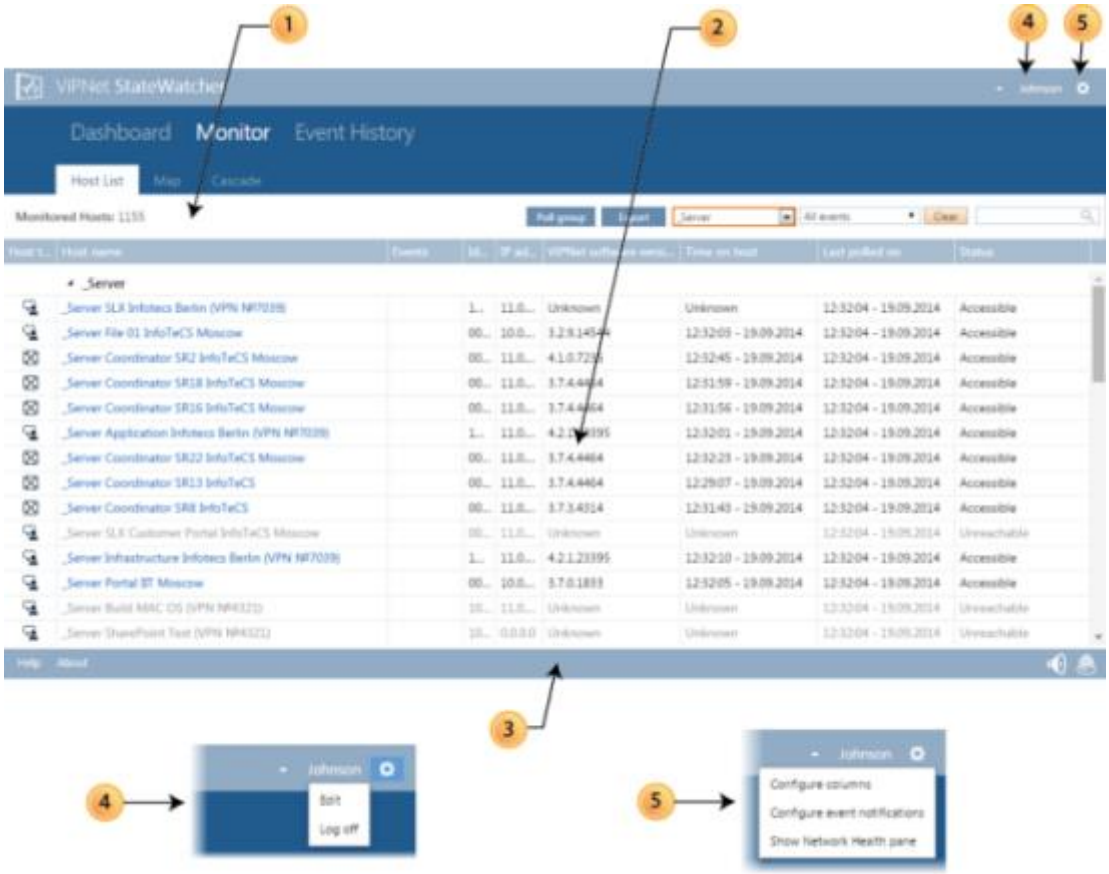

Figure 12: Host List page

The following elements are marked with numbers in the figure:

1 The toolbar containing filters for monitored hosts search. On the left side of the toolbar, the number of monitored hosts that has been added for monitoring on this Monitoring Server is shown. These hosts may be polled or not.

2 The view pane that includes a list of monitored hosts with their detailed information.

3 The notification pane containing the following buttons and links:

- **Help** for starting the context help.
- **About** for viewing information about the ViPNet StateWatcher.

- **Configure event notifications** for configuring notifications about host events in a dialog box.
- for turning sound notifications on and off.
- for information about events registered on monitored hosts.
- for notification about the export of unprocessed host parameters.
- for notification about the export of events history.

4 The **User** menu, allowing you to edit your account or exit the monitoring system.

5 The **Settings** menu, allowing you to choose which columns will be displayed in the hosts list, to configure pop-up messages, and to show or hide the Network Health panel.

2

ViPNet Host Monitoring

Monitoring Hosts in the Host List	29
Monitoring Hosts on a Dashboard	38
Monitoring Hosts on a Map	45
Viewing the Monitoring Events History	52
Exporting Unprocessed Host Parameters	57
Working with Notifications	60
Statistics	67
Monitoring the Network Health	71

Monitoring Hosts in the Host List

You may monitor hosts in the host list. Monitoring is a necessary procedure for getting detailed actual information about ViPNet hosts.

Viewing the Monitored Hosts List

To view the host list, on the main page, on the **Monitor** tab, click **Host List**. On this tab, there is a list of grouped hosts with the polling results for each host, and also links and buttons for starting functions available for the user. If this monitoring server has cascaded child servers, then, on the **Host List** page, cascaded monitored hosts will be displayed as well.

Monitored Hosts List

A list of monitored hosts includes only the monitored hosts specified by the administrator of this monitoring server.

For each monitored host, the following information is displayed:

Table 5: Columns of the Monitored Hosts list

Column name	Description
ViPNet type	Host type icon. Monitoring Server detects it automatically when adding the host for monitoring.
Host name	The name of the ViPNet host or the public host
Events	Events registered on the monitored host. In the **Events** column, you can see the number of events and a colored icon indicating the most important event registered on a host during a poll. An icon color depends on the Monitoring Server program settings.
Identifier	The identifier of the ViPNet host.
IP address	The current IP address of the monitored host.
ViPNet software version	The version of the ViPNet software installed on a ViPNet host.
Host local time	The local time and date on a monitored host.
Last time polled	The time and date of the last poll of a monitored host. The Monitoring Server polls hosts periodically, and the poll period can be defined in the program settings. You

	can initiate polling process manually any time you want (to do this, select the required hosts and click **Poll**).
Status	The current status of a monitored host with the ViPNet Monitor program installed. There are two possible statuses: Accessible and Unreachable.

Note: The **ViPNet software version**, **Host local time**, and **Last time polled** parameters are not automatically displayed for the list of cascaded monitored hosts. They can be received only on request of the parent monitoring server's administrator.

You may sort the information in the list of monitored hosts by any column, except for the **Events** column, by clicking the column header. On the first click, the information is sorted in ascending order, on the second click, it is sorted in descending order.

Note: You can sort only hosts in a group, but not in a whole list.

You can adjust the width and order of columns in the list of monitored hosts:

- To change the width of a column, hover over the column header's border, and then click and drag the border to stretch or narrow the column.
- To change the order of columns in the monitored hosts list, click the column header, drag, and drop it.

You may add or remove columns displayed in the list of monitored hosts. To do this:

1 On the **Host List** tab, in the upper-right corner, click **Settings**, and then choose **Configure columns**.

Figure 13: Configuring columns in the list of monitored hosts

2 An **Add/Remove Columns in the Table** window will appear, where you can add or remove columns from the monitored hosts list with the and buttons.

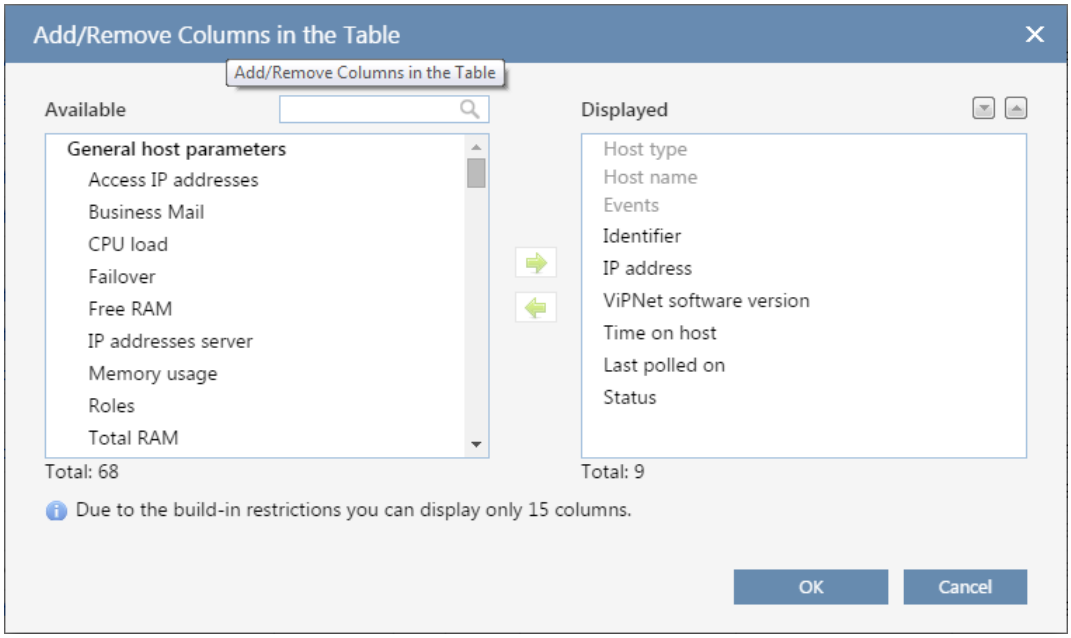

Figure 14: Configuring which columns should be displayed in the list of monitored hosts

---

Note: The **Type**, **Host name**, and **Events** columns are always displayed. You can't remove them from **Displayed**.

In the window for adding and removing columns, parameters of both ViPNet hosts and public hosts are displayed. Thus, for the ViPNet hosts, the public hosts' parameters will have the **Unknown** status. The same applies to ViPNet hosts' parameters for public hosts.

---

3 After you finish choosing the columns to be displayed, click **OK**. To discard the changes, click **Cancel**.

As a result, the required information about the monitored hosts will be displayed in the list. These settings will be applied in the ensuing sessions on your host where you use Monitoring Web Access.

Host Groups

Hosts in the list are grouped according to the current Monitoring Server settings.

You may expand and collapse any of the groups. To do this, use the arrow button to the left of the group name.

In the pane with a group name, on the right, there is information about the number of events that have occurred on the hosts of the current group. If you need, you may filter the hosts in a group by events tracked on them.

Only the administrator can change settings for groups. Besides the groups specified by the administrator, in Monitoring Web Access, there are the following pre-defined groups:

- **Default group** is a group containing all monitored hosts that are not included in other groups.

  This group is always displayed in the list of monitored hosts.

- **Cascaded hosts** is a group of hosts monitored by child servers of your monitoring server in a cascade hierarchy.

  Hosts from this group are not monitored by your server directly. They are monitored by your server's child monitoring servers.

  This group is included in the monitored hosts list only if the monitoring server has any child monitoring servers in a cascade.

Viewing Information about a Monitored Host

To view information about a host, click the link with the host's name. As a result, the **Host Information** window will be displayed with complete information about the host.

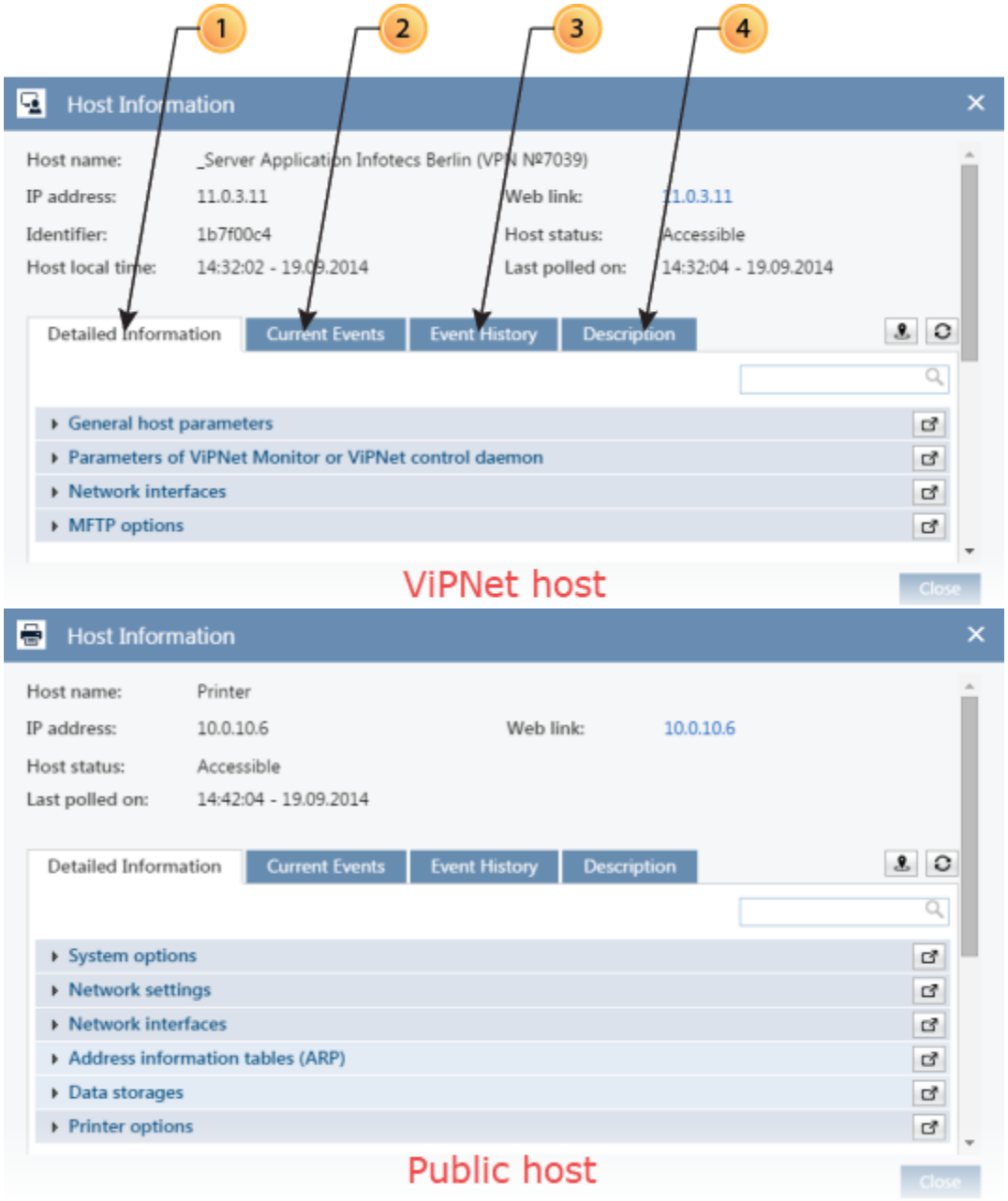

Figure 15: Viewing information about a monitored host

On top of the window, you can see general information about the monitored host, including its name, ViPNet identifier, IP address, and the web link. Also, the host's status, time and date of the last poll, and local date and time on the host are displayed here. On top of the public host's information window, the host's name, web link, IP address, state, last poll date and time are displayed.

The parameters on top of the window are updated every time the host is polled, whether automatically or manually.

To update information in the **Host Information** window, click **Poll**. For detailed information about a host, click the corresponding tab.

To find a host on the map, click **Locate on the map**. This button is displayed only if a Monitoring Server administrator has added the host to the map.

The following elements are marked with numbers in the figure:

1. The **Detailed Information** tab includes complete information about the host and its parameters. For the complete list of the parameters and their description, see the Appendix (see Parameters Monitored on Hosts on page 89). The detailed information tab is not updated dynamically while the host is being polled. To update this information, close and reopen the **Host Information** window.

2. The **Current Events** tab shows event notifications received from the host. The current notifications (the notifications that were created by processing rules) are displayed with the corresponding executed processing rules. The parameters on this tab are updated every time the host is polled, either automatically or manually.

   On this tab, you can also disable notification about this host by clicking **Suspend notifications**. In the list, choose the time interval (1 hour, 12 hours, 1 day). During this time interval, the events in the **Events** column will not be changed, and the **Suspend notifications** button will be replaced with the **Resume notifications** button. You can resume displaying the notifications (before the end of suspending time interval) by clicking this button. Notification on maps is also disabled.

3. The **Events history** tab contains history of processing rules executions for the host. for the last 24 hours.

4. The **Description** tab allows you_ to save arbitrary information about a host (for example, if you want to give a detailed description of a host). The added information can be viewed and edited by other users.

Note: If no events registered before are displayed on **Events History** tab, contact your monitoring server administrator. They could be removed by the data rotation procedure (see Data rotation on page 122).

Viewing Information about the Events Registered on Hosts

To view the information about the events registered on monitored hosts:

1. On the **Host List** page, in the notification pane, click .

   In the **Information about events registered on hosts** window, you can get information about events registered on monitored hosts (see Pop-up Messages on page 61).

2. If necessary, you may also get detailed information about each registered event. To do this, choose the required event from the list and, in the **Event** column, click the icon of the corresponding severity level. The window with the information about the host where the event was registered will be displayed.

Polling Monitored Hosts

The **Hosts list** page is refreshed automatically every time the monitoring server polls the hosts. If the monitoring server does not receive any information about a parameter, then this parameter is considered to be unknown. In this case, the word **Unknown** is displayed instead of this parameter.

The list of cascaded monitored hosts is updated automatically in the following cases:

- You add a new host to the list of monitored hosts on a child monitoring server.
- You remove a host from the list of monitored hosts on a child monitoring server.
- You establish a connection to a new child monitoring server.

The monitoring server polls hosts periodically. You specify the poll time period in the program settings. However, you may initiate polling of all or some monitored hosts manually at any time. To do this:

1. On the **Hosts list** page, on the toolbar, click **Poll group**.
2. In the **Poll Hosts** window, move hosts or host groups from the left list to the right list and click **Poll**.

As a result, information about the state of the selected hosts will be updated.

To poll the monitored hosts cascaded by a child monitoring server, complete the above-described actions or click next to the child monitoring server name in the **Cascaded hosts** group (all hosts cascaded by this server will be polled).

After the Monitoring Server program restarts, for every host, parameters received during the last successful poll are displayed. After a host is polled, its parameters are updated to reflect its actual state. For example, suppose that a monitored host had been turned off before Monitoring Server stopped working, and this computer's parameters were unknown. So, after Monitoring Server starts, it displays the host parameters received during the last successful poll. Only after the next poll the parameters values are changed to **Unknown**.

Filtering Monitored Hosts

Monitored hosts filtering is intended for quick search of the monitored hosts by the specified parameters.

For easier viewing, you can filter hosts in one of the following ways:

- Filtering hosts in a group.

  On the **Host List** page in the pane with the group name, click the link with the number and severity of events. The page will be displayed with all hosts in the selected group, on which the events of the selected severity level were registered. You may cancel searching by the selected criteria by clicking the **Default** button on the toolbar.

  By default, the severity levels are marked in red, yellow, and green colors for Critical, Warning, and Standard severity levels. Informational messages are marked in blue color.

Default group						
Drozdov Yury senior ...		0001081d	11.0.3.97	Unknown	Unknown	20:28:31 - 16.01.20...
Bondar Vladimir TDC I...		0001064b	11.0.1.21	Unknown	Unknown	20:28:31 - 16.01.20...
Bazanova Vera Logisti...	1	0001070b	11.0.1.94	3.2.9.11025	20:29:42 - 16.01.20...	20:28:31 - 16.01.20...
Bystrov Evgeny Sales ...		00010896	11.0.3.243	Unknown	Unknown	20:28:31 - 16.01.20...
Borodin Mikhail Mana...		00010748	11.0.1.124	Unknown	Unknown	20:28:31 - 16.01.20...
_Server Coordinator S...		0001027d	10.0.2.20	4.0.1.4831	20:29:18 - 16.01.20...	20:28:05 - 16.01.20...
CSI, Nastya Shpilevska...		10e10a0b	11.0.3.202	3.2.10.15632	20:29:43 - 16.01.20...	20:28:31 - 16.01.20...

Figure 16: Filtering hosts in a group

- Hosts filtering by monitoring groups.

  Select the check boxes of the groups you want to display and then click **Apply**.

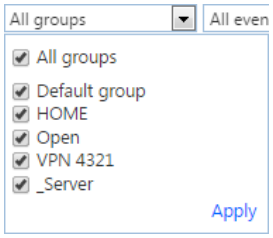

Figure 17: Filtering hosts by groups

- Filtering by event severity levels.

  On the toolbar, in the **All events list**, choose the event severity level you want to view You may use only one of the existing filters at a time.

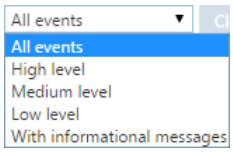

Figure 18: Filtering hosts by a severity level

- Filtering hosts by using a search request.

  To do this, on the toolbar, in the Search box, type the name or a part of the name of the required host. Every time you type a symbol, automatic list filtering is performed according to occurrence of the typed characters in the **Host name** column. To clear the search box, click the ✕ icon.

Warning: Search requests are not case sensitive.

Monitoring Hosts on a Dashboard

To acquire up-to-date information about monitored hosts in a convenient form you can configure a dashboard that will only display the parameters you are interested in. For example, if your organization has mission-critical servers, and it is important for you to get the latest information about their condition, you can create a Dashboard with the appropriate settings and monitor the status of these servers.

A dashboard opens as a home page after user authentication. Dashboard is displayed in one or more tabs (depending on settings). Each tab can contain up to six different types of tiles (for example, the current values of the parameters, or a map).

When a new user account is created, a default dashboard is also created for it (**Home** tab). It contains the following information tiles:

- **Current settings**,
- **Graph**,
- **Recent events,**
- **Map**.

When working with MWA, you can configure a default monitoring dashboard default or create a new one. You can configure up to eight dashboards (including the default dashboard) for each user. Dashboard and its settings are individual for each user and are not displayed to other users.

The figure below shows a default dashboard.

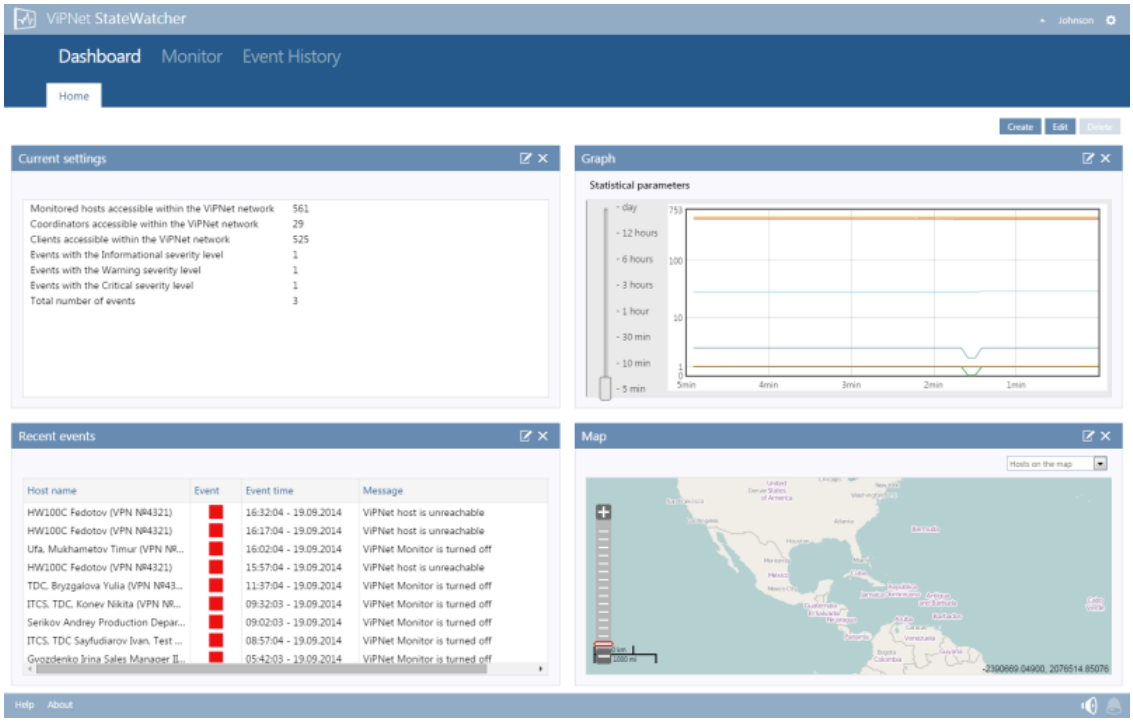
ViPNet StateWatcher
Johnson
Dashboard
Monitor
Event History
Home
Create
Edit
Delete
Current settings
Monitored hosts accessible within the ViPNet network 561
Coordinators accessible within the ViPNet network 29
Clients accessible within the ViPNet network 525
Events with the Informational severity level 1
Events with the Warning severity level 1
Events with the Critical severity level 1
Total number of events 3
Graph
Statistical parameters
- day
- 12 hours
- 6 hours
- 3 hours
- 1 hour
- 30 min
- 10 min
- 5 min
Recent events
Host name
Event
Event time
Message
HW100C Fedotov (VPN NR4321) 16:32:04 - 19.09.2014 ViPNet host is unreachable
HW100C Fedotov (VPN NR4321) 16:17:04 - 19.09.2014 ViPNet host is unreachable
Ufa. Mukhametov Timur (VPN NR... 16:02:04 - 19.09.2014 ViPNet Monitor is turned off
HW100C Fedotov (VPN NR4321) 15:57:04 - 19.09.2014 ViPNet host is unreachable
TDC. Bryzgalova Yulia (VPN NR43... 11:37:04 - 19.09.2014 ViPNet Monitor is turned off
ITCS. TDC. Konev Nikita (VPN NR... 09:32:03 - 19.09.2014 ViPNet Monitor is turned off
Serikov Andrey Production Depar... 09:02:03 - 19.09.2014 ViPNet Monitor is turned off
ITCS. TDC Sayfudiarov Ivan. Test ... 08:57:04 - 19.09.2014 ViPNet Monitor is turned off
Gvozdenko Irina Sales Manager II... 05:42:03 - 19.09.2014 ViPNet Monitor is turned off
Map
Hosts on the map
Help
About

Figure 19: Default dashboard

Configuring Dashboard

To create a new dashboard:

1. Go to the **Dashboard** page and on the toolbar click **Create**.
2. In the displayed window, specify the name of the panel and the location of the tiles. There can be no more than six tiles. To save the settings, click **Save**.

Note: To configure an existing dashboard select the desired tab, and on the toolbar click **Edit**.

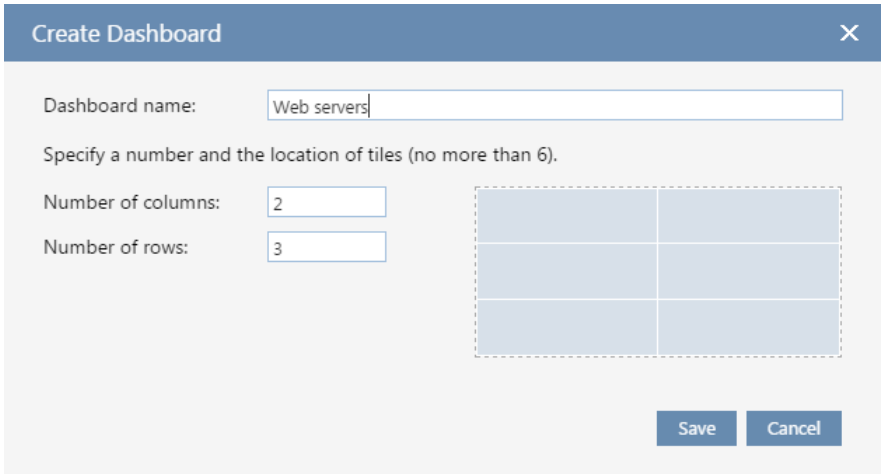

Figure 20: Configuring a dashboard

You will see a new dashboard with a number of tiles that you entered before.

3 To configure an information tile, in the new dashboard click the desired tile. To configure a tile in an existing dashboard, click tab and in the upper part of the information tile click **Edit**.

4 If you want to keep track of the current parameters of any hosts, select the **Current settings** tile type. For details see Configuring a Current Settings Tile (on page 41).

5 If you want to keep track of the changes in any parameters in the form of a graph, select the **Graph** tile type. For details, see Configuring a Graph Tile (on page 42).

6 If you want to track the latest detected monitoring events, select the **Recent events** tile type. If you want to keep track of all parameters, use the default settings. If you want to select monitoring hosts, select the **Use filter** check box, and select the required nodes. If you want to monitor only the events of particular importance, check the boxes next to the required critical levels. To save the settings, click **Save**.

7 If you want to keep track of the hosts on a map, select the **Map** tile type and click **Save**.

As a result the following dashboard will be created.

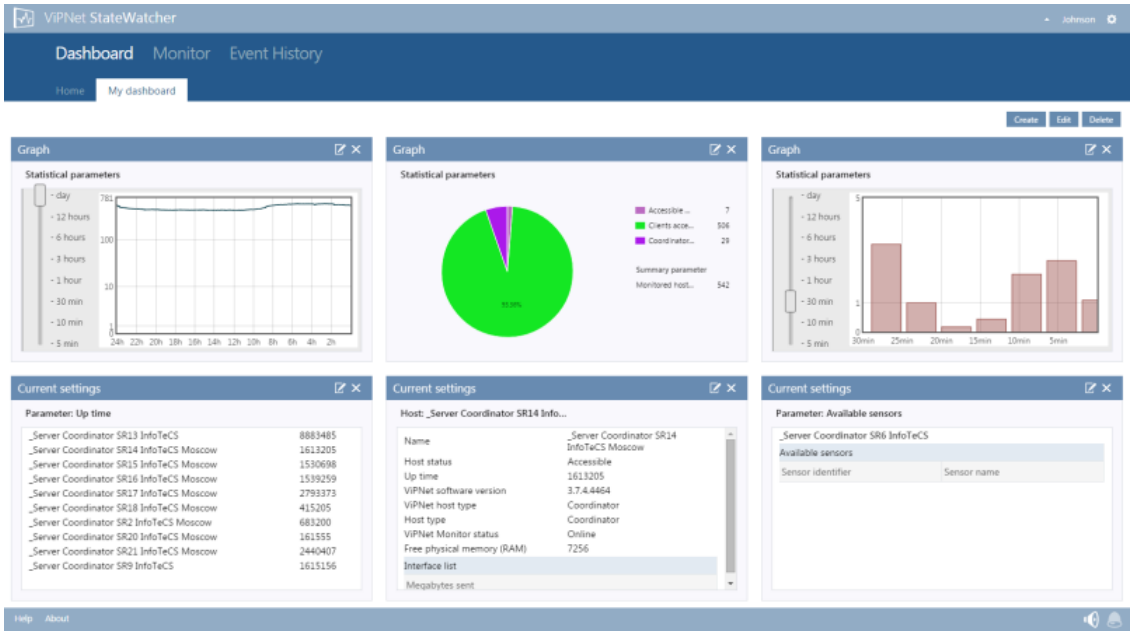

Figure 21: An example of a configured dashboard

Configuring a Current Settings Tile

If you want to keep track of the current parameters of any hosts, select the **Current settings** tile type. To do this:

1. To configure an information tile in the new dashboard click the desired tile. To configure a tile in an existing dashboard, select the tab and in the upper part of the information tile click **Edit**.
2. Select the **Current settings** tile type.
3. If you want to view the value of a particular parameter for several hosts, in the **Filter using** list choose **Parameter**. In the list of parameters choose a parameter that you want to monitor, in the list of hosts select the check boxes next to the desired hosts.
4. If you want to view the value of a particular parameter for several hosts, in the **Filter using** list choose **Parameter**. In the list of parameters choose a parameter that you want to monitor, in the list of hosts select the check boxes next to the desired hosts.
5. To monitor statistic parameters in an information tile, select **Statistic parameters** in the **Filer using list**. Statistical parameters allow to visually monitor the current state of a ViPNet network. For more information about the statistical parameters, see Monitoring the Network Health (on page 71).

6 If you want to see the time of the last update of the parameters values, select a check box next to **Show update time**.

7 To save the new filter's parameters, click **OK**.

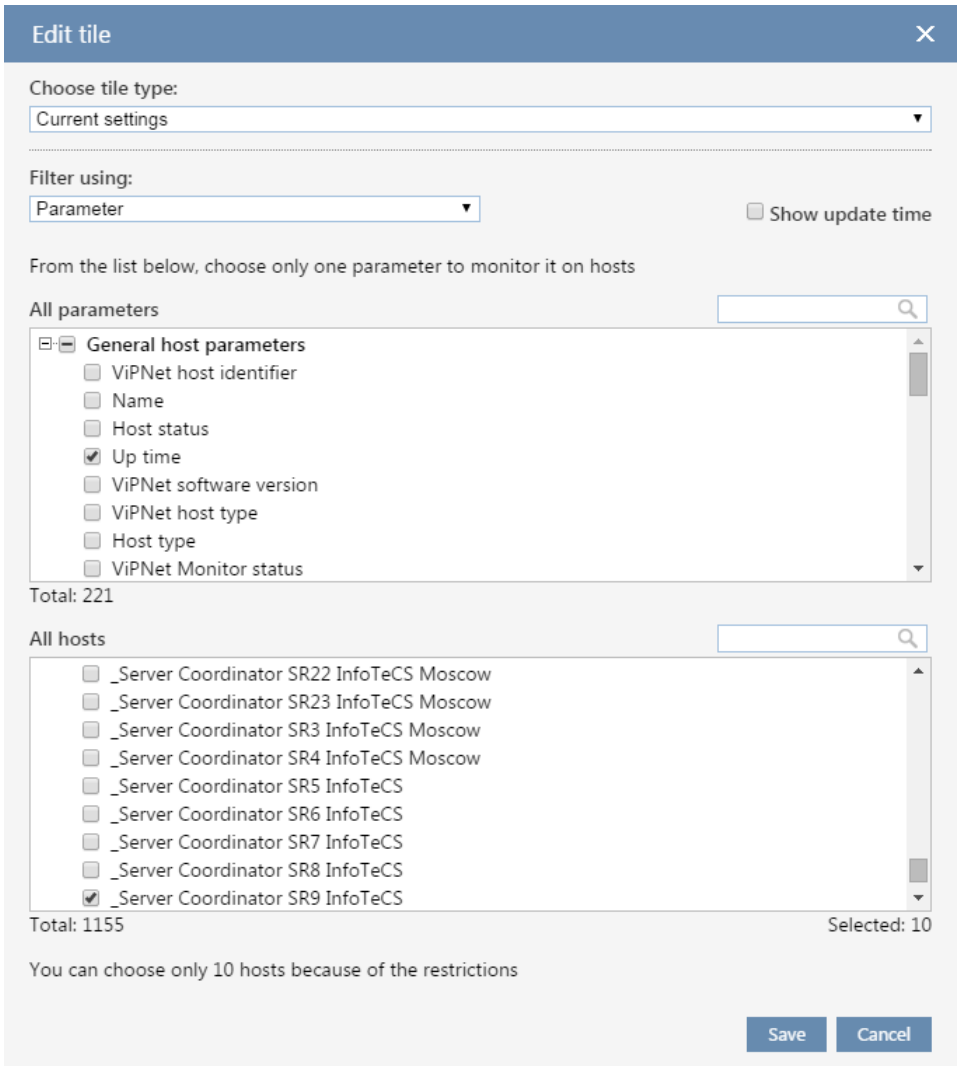

Figure 22: Configuring dashboard

Configuring a Graph Tile

To display the parameters as a graph you can configure the **Graph** tile type. To do this, follow these steps:

1 To configure an information tile in the new dashboard click the desired tile. To configure a tile in an existing dashboard, select the tab and in the upper part of the information tile click **Edit**.

2 Select the **Graph** tile type and a graph type: line chart, pie chart, or bar chart.

3 If you want to view the value of a particular parameter for several hosts, in the **Filter using** list choose **Parameter**. In the list of parameters choose a parameter that you want to monitor, in the list of hosts select the check boxes next to the desired hosts.

4 If you want to view the value of a particular parameter for several hosts, in the **Filter using** list choose **Parameter**. In the list of parameters choose a parameter that you want to monitor, in the list of hosts select the check boxes next to the desired hosts.

5 To monitor statistic parameters in an information tile, select **Statistic parameters** in the **Filer using list**.

6 If you want to see the time of the last update of the parameters values in a tile with a **Pie chart** type, select a check box next to **Show update time**.

7 If necessary, change the graph color. To do this, press the palette button next to the corresponding parameter and select a color.

8 If you selected a **Pie chart** type, you can select, which parameter will be a summary parameter. Percentages of the other parameters will be calculated with respect to the summary parameter (for example, when monitoring the space on a hard drive, select the total disk size as a summary parameter). The final parameter should be greater than the other selected parameters, otherwise a graph might not be displayed correctly.

Note: It is recommended to use a summary parameter. Using a summary parameter allows you to correctly display the percentages of the other parameters in case if the data is missing for one of the parameters.

9 After you configure the graph parameters, click **Save**.

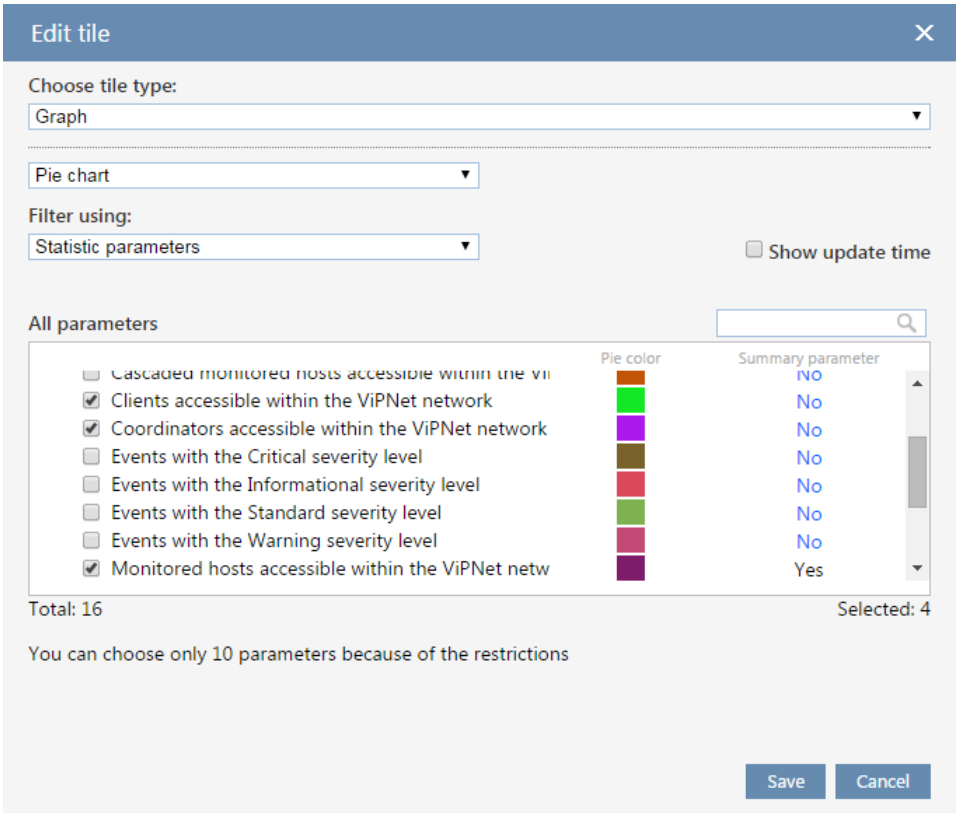

Figure 23: Configuring dashboard

Monitoring Hosts on a Map

You can monitor the host state not only in the monitored hosts list, but also on a geographical map. In the main window, on the **Monitor** tab, click **Map**. On this page on a geographical map you can view monitored hosts according to their geographical location. The administrator adjusts hosts' location on a map while configuring the Monitoring Server program.

Note: On a map, you can view both directly monitored hosts and hosts monitored by child servers in a cascade.

You can manually poll all hosts or several hosts on a map. To do this:

1. On the toolbar, click **Poll group**.
2. In the **Poll Hosts** window, move hosts or host groups from the left list to the right list and click **Poll**. As a result, information about the state of the selected hosts will be updated.

There are several types of maps supported by the ViPNet StateWatcher software. The displayed type depends on the customization pack (on page 122). The standard customization pack includes the following maps:

- Russian Federation map stored locally on the server (it is displayed by default when you start maps for the first time).
- OpenStreetMap online map.

To switch to another map, choose the required one from the map types list.

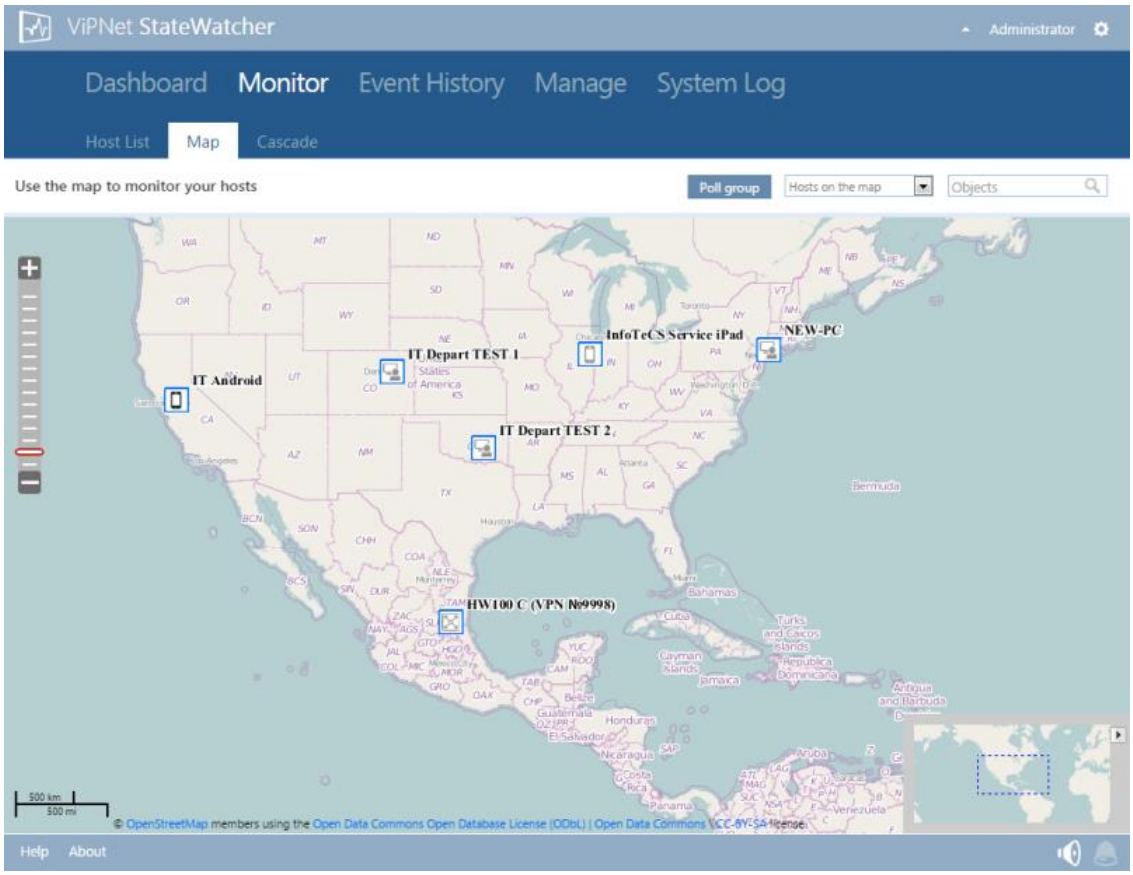

Figure 24: Viewing hosts on a map

Hosts are indicated with different icons on a map depending on the host's type:

- means a protected host with installed ViPNet Client software;
- means a protected host with installed ViPNet Coordinator software or with ViPNet Coordinator HW/VA;
- means a protected mobile host (a smartphone) with a special version of the ViPNet Client software;
- means a protected host with ViPNet ThinClient;
- means a public host;
- means a uninterruptible power supply;
- means a printer;
- means a router;
- means an IDS;
- means a public host;

means a group of hosts. It is displayed in case you set district-based displaying of hosts.

Blinking of the icons denotes that some events are detected on the hosts (for example,). When configuring the monitoring server, the administrator sets the color of blinking for each severity level. For more information on map notification, see Notifications on the Map (see Visual notification on the Map on page 64).

When working with a map, you can:

- Scaling the map with the ability to set the default zoom level.
- Moving around the map and positioning on it (see Recentering the Map and Positioning on the Map on page 47).
- Searching for a monitored host by its name and automatic centering on the search result (see Searching for Hosts on the Map on page 48).
- Searching for a geographical object by its name and automatic centering on the search result (see Searching for Geographical Objects on page 49).
- Acquiring information about a monitored host and disabling notification (see Viewing Information about a Monitored Host on page 50).
- Customize display styles for different types of objects, and types of hosts for different zoom levels.

All user-defined map settings are saved by the Monitoring Server program and applied on the next user logon, for instance, zoom and position. When you open the map for the first time, it is displayed fully with default display settings.

Recentering the Map and Positioning on the Map

To view a certain area on the map:

- Click and hold the map, dragging it in the required direction.
- On your minimap in the lower-right corner of the page, click and hold the viewport and drag it in the required direction.

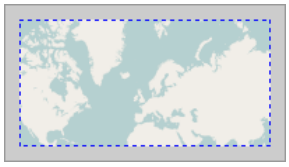

Figure 25: The minimap

On the map, you can recenter and zoom in at a certain country, region, or another geographical object by double-clicking it. As a result, the clicked object will be zoomed in and displayed in the center of the map.

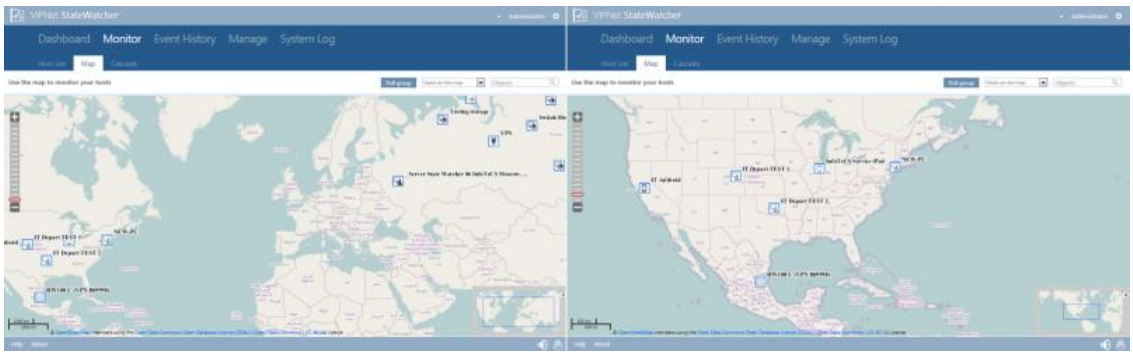

Figure 26: Positioning on the map

When you search for a monitored host or a geographical object, the map is automatically recentered at the host (see Searching for Hosts on the Map on page 48) or object (see Searching for Geographical Objects on page 49).

Searching for Hosts on the Map

To find a monitored host:

1. On the **Monitor** tab, click **Map**.
2. On the toolbar, expand the **Hosts on the map** list and choose the required host. You can also type one or more characters to filter this list.

   Case-insensitive filtering will be performed, and the hosts' names containing the typed characters will be displayed. After you have chosen the host, it is automatically positioned on the map.

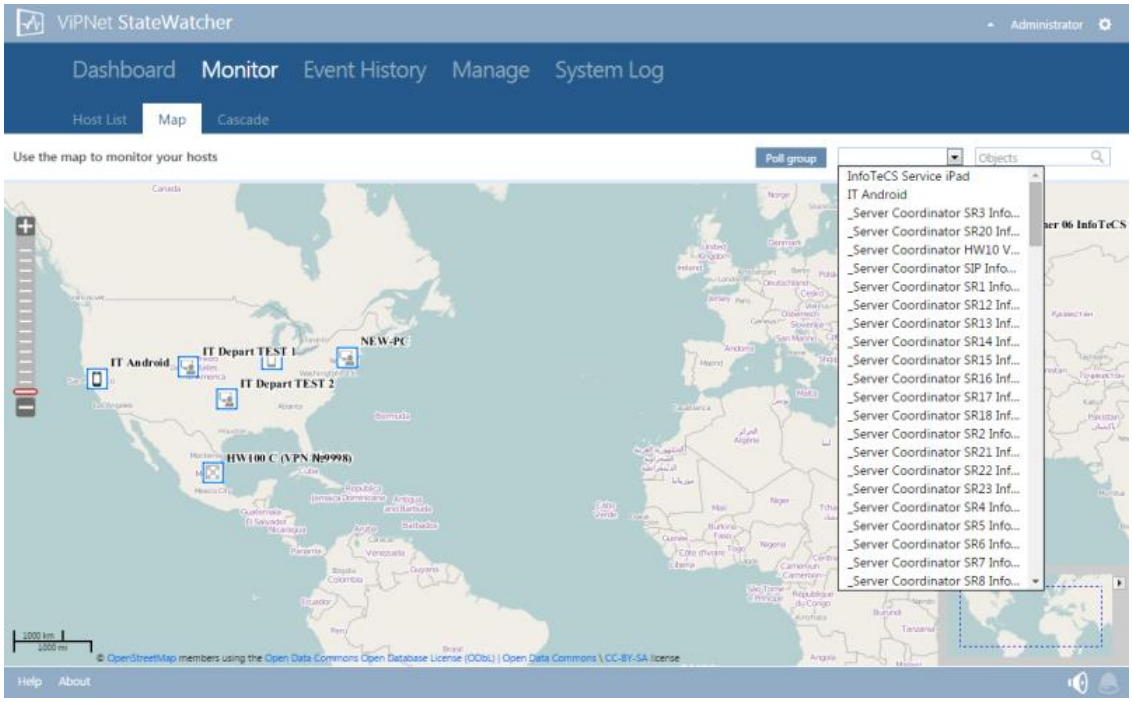

Figure 27: Search for a monitored host on the map

Searching for Geographical Objects

To search for a geographical object on an online map:

1. On the **Monitor** > **Map** page, display OpenStreetMap.
2. In the search box, type the geographical object's name and press **Enter** or click **Find**.

   As a result, the **Search results** window will be displayed, containing the objects found on the query with OpenStreetMap Nominatim. OpenStreetMap Nominatim is a tool for finding geographical objects in OpenStreetMap database.

   The search results are displayed as soon as the objects are found.

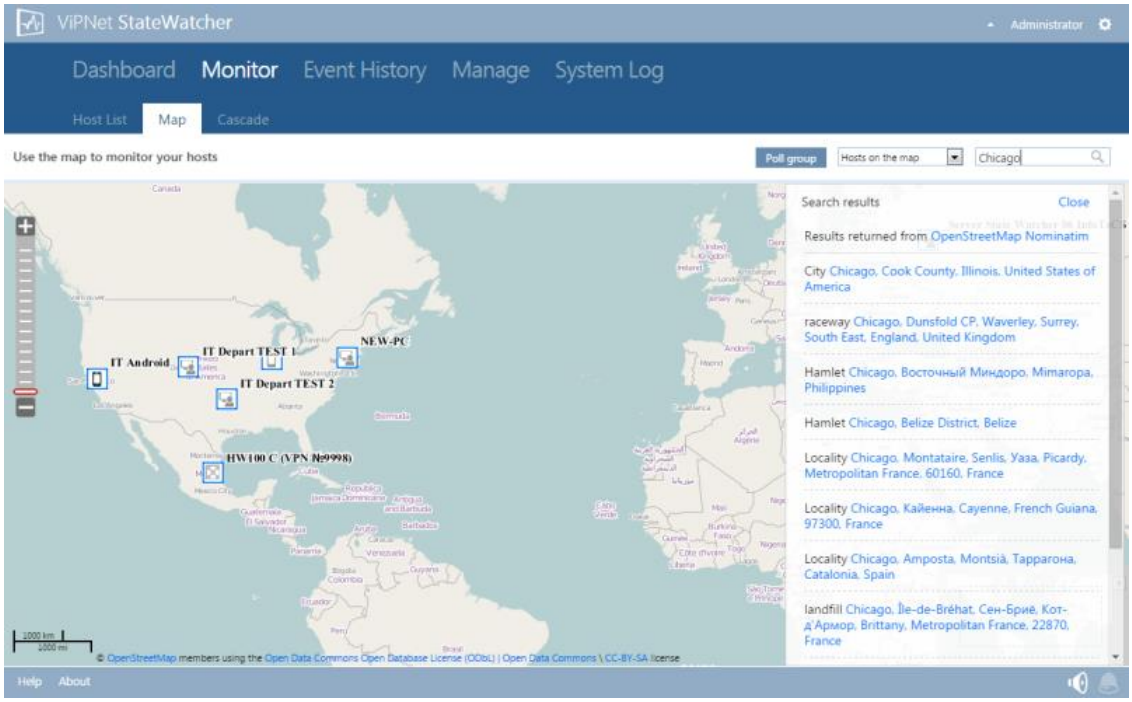

Figure 28: Search for an object on the map

3 Click the link with the required object's name. The online map will be recentered according to the object's location.

Viewing Information about a Monitored Host

To view information about a monitored host, click this host on the map. The host information window will be displayed (see Viewing Information about a Monitored Host on page 32).

- If some events are registered on the host, then the **Current Events** tab of the **Host Information** window will be displayed.
- If no events are registered on the host, the **Suspend notifications** button will be unavailable, and the **Detailed Information** tab of the **Host Information** window will be displayed.

Viewing Information about a Monitored Hosts Group

To view information about a group of monitored hosts:

1 Click the group's icon on your map.

2 In the **Hosts** window, on the list, click the host's name. The information window will be maximized.

By default, all the windows are minimized.

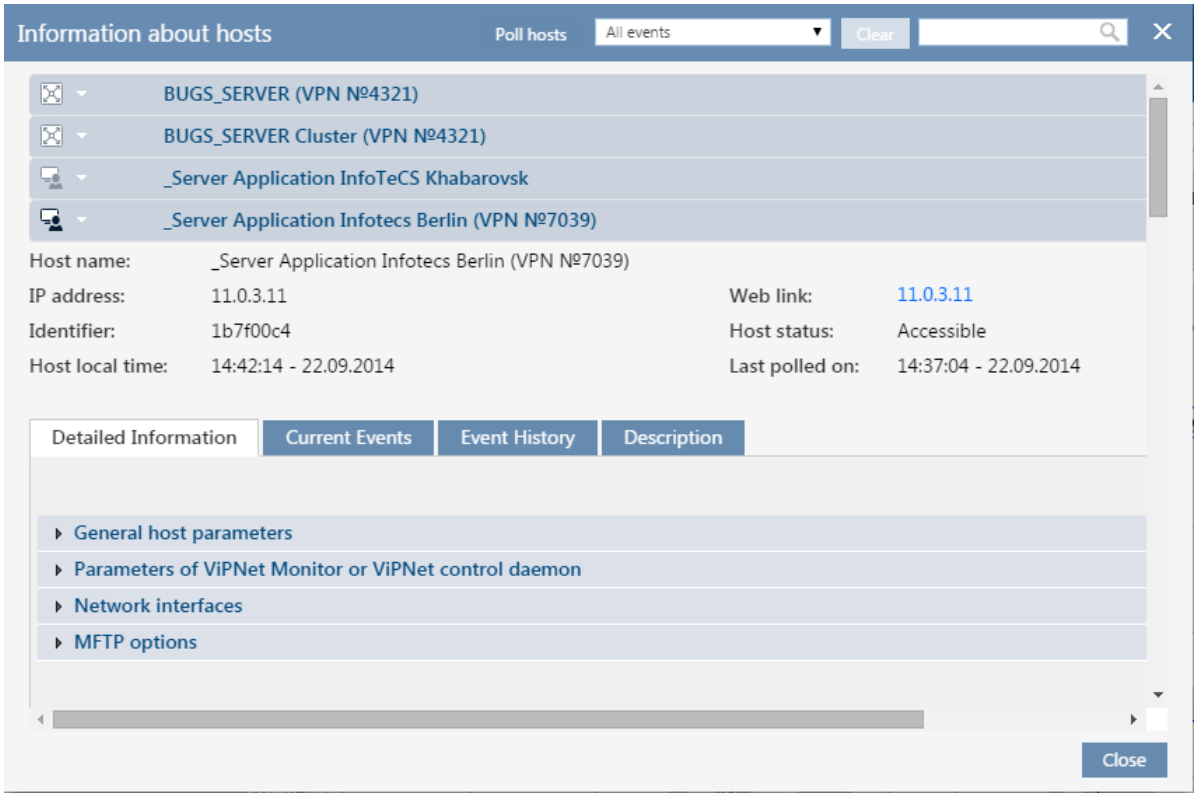

Figure 29: Viewing information about the events registered on hosts

Viewing the Monitoring Events History

The Monitoring Server program saves the history of the monitoring events registered by the monitoring system. By viewing monitoring events, you can learn about the events registered since the system has started, and, if necessary, export these events to other software. All the events registered when the rules are executed are added to the monitoring system database, including:

- **Host name**, the name of a monitored host on a ViPNet network.
- **Event time**, the time of the event detection.
- **Processing rule name**, the name of a processing rule.
- **Event severity level**, an event's severity level.
- **Message**, a message from the Monitoring Server program about the registered event.

Note: If a rule is executed to several hosts, then Monitoring Server will register several events, and each event entry will be saved separately.

To view monitoring events history:

1 On the main page, click the **Events History** tab.

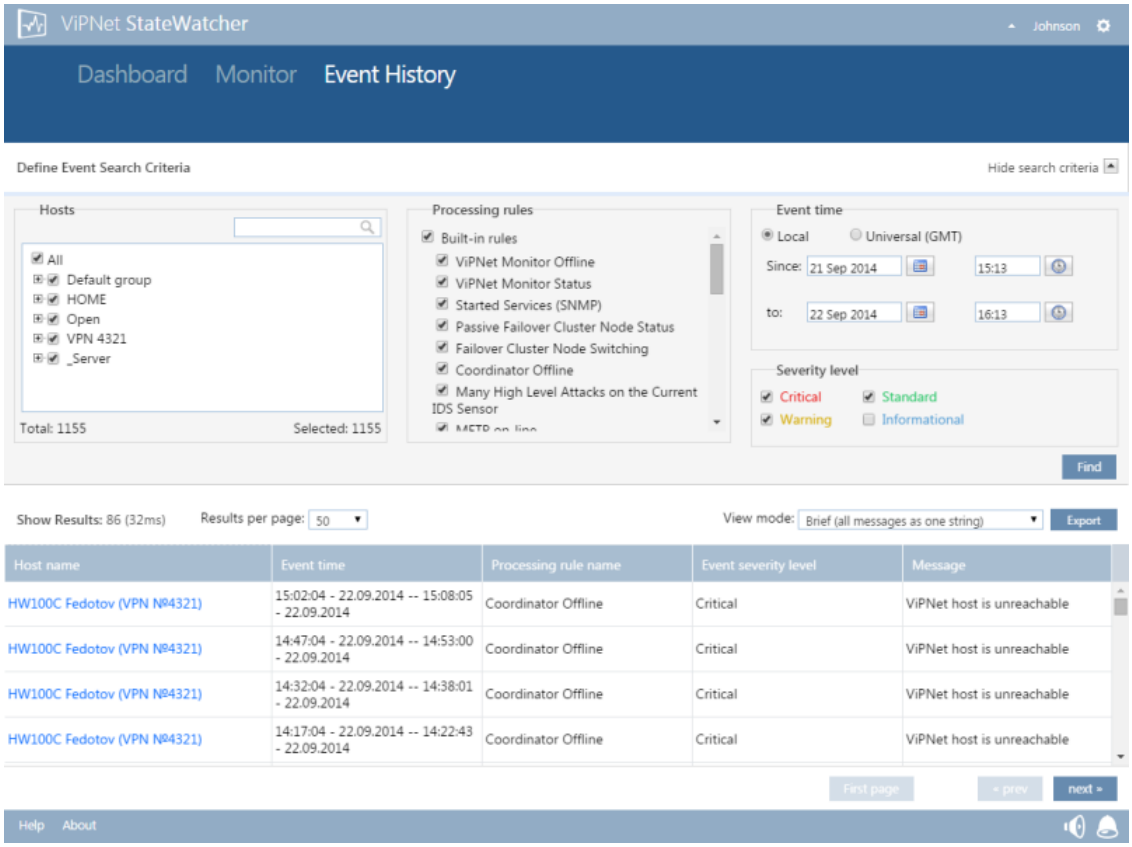

Figure 30: Viewing monitoring events history

2 On the **Search criteria** page, specify filtering parameters for the events registered by the monitoring system and click **Find**.

A list with the events selected from the database according to your filtering parameters will be displayed.

3 In the **Results** field, the number of the events found and the search time will be shown. When you browse another page with search results, the time shown may also change according to the quantity of the entries found. By default, there are 50 results on the search results page.

If necessary, you may change the number of results on the page. To do this, in the **Number of entries per page** list, choose the number you want. To list through search results pages, click the « prev next » buttons.

If an entry is displayed in gray, it refers to events registered by the rules that are now deleted.

By default, the entries on the list are sorted by the time the processing rule was executed (the **Detection time** column) in descending order.

4 If you want to sort the event list by any other column, click the title of this column.

You can export the resulting events list to a file (see Exporting the Monitoring Events History on page 55).

Detailed Viewing of the Monitoring Events History

When viewing monitoring events history, you may obtain detailed information about any of the events.

To do this:

1 On the main page, click the **Events History** tab.

2 Specify event search criteria and click **Find**.

3 In the **Results** list, click the entry with the event you need.

4 In the **Detailed information about event** window you will find the following information about the monitoring event:

- **Host**, a monitoring ViPNet host name.
- **Path in the cascade**, a chain of the child monitoring servers through which the monitoring event notification was transferred. This field is displayed only for the events registered on cascaded monitored hosts.
- **Detection time**, a time when an event was detected by the system.
- **End time**, a time when an event ended. If the event has not been ended the box is empty.
- **Message**, an informational message about the registered event.
- **Processing rule**, a processing rule name.
- **Parameters**, the host parameters that caused the rule execution.

  The parameters are shown in a table, where:

  - **Name**, a name of a changed parameter.
  - **Current**, the current value of this parameter.
  - **Previous**, a parameter value obtained during the previous poll.
  - **The last available**, a value obtained during the last successful poll. Opposite to the previous value that can be unknown, this parameter has a real value.

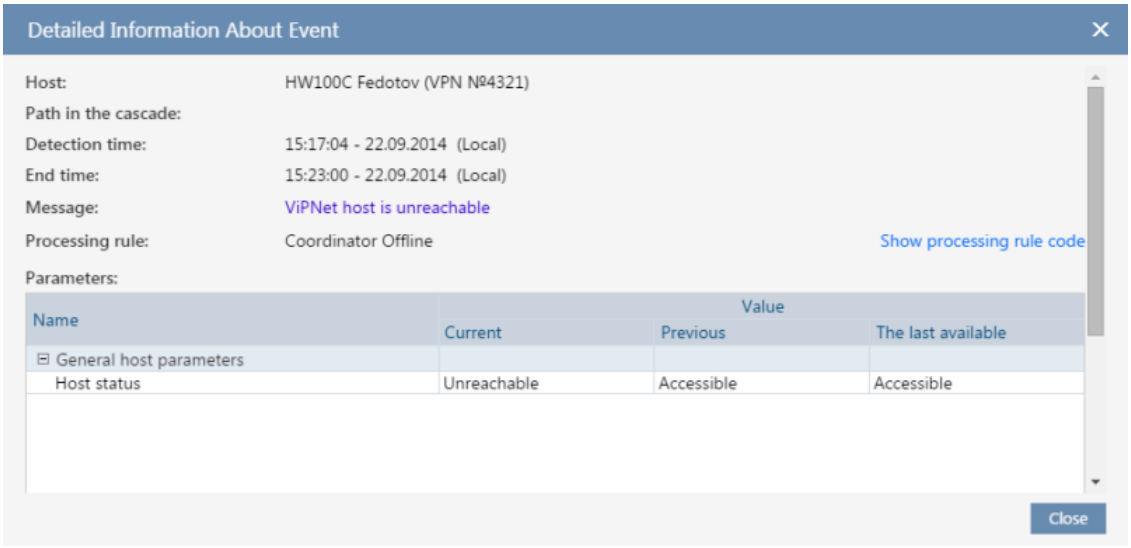

Figure 31: Viewing detailed information about an event

To view the settings of the processing rule according to which an event was registered, in the **Detailed Information** window, click **Show processing rule code**.

For more information about the processing rules structure, see the document "ViPNet StateWatcher 4.3: Monitoring System for ViPNet Networks. Monitoring Server. Administrator's Guide."

5 When you have finished viewing the detailed information, click **Close**.

6 After that, you can return back to the monitored host list. To do that, on the **Monitor** tab, click **Hosts List**.

Exporting the Monitoring Events History

The monitoring events history entries filtered by parameters that you specify can be exported to a file that then can be imported to other software (for example, to Microsoft Office).

Warning: The exported monitoring events history file can be then imported to Microsoft Office Excel or Open Office Calc. To import monitoring events to a program, you must take into account the specifications and limitations of this program. The importing may take you about 20 minutes, depending on your computer specifications.

The Monitoring Server program exports event history in the background, allowing you to work with the monitoring system while it performs the export.

To export monitoring events history to a file:

1. On the main page, click the **Events History** tab.
2. Specify event search criteria and click **Find**.
3. In the search results pane, click **Export**.

   An exporting process will start. During this process, in the notification pane, the icon will be displayed. When the exporting process will be finished, the icon will be displayed.
4. Click . The window prompting you whether an export file should be saved will be displayed. In the request window, click **OK**.

   If you export over 60,000 entries about monitoring events, you will be prompted that the created file can't be opened with Microsoft Office Excel.

Note: For the export file to be available for opening with Microsoft Office Excel, you should decrease the entries number to 60,000. To do this, narrow the events filtering criteria.

5. The resulting file will be saved as an archive (a file with a `.zip` extension):

   This archive includes a file with an `.xml` extension, to where the selected monitoring event history entries are saved. The following data (see Structure of the Events History Export File on page 86) is saved to an export file:

   - monitored host identifier;
   - monitored host name;
   - time and date of a processing rule execution;
   - processing rule identifier;
   - processing rule name;
   - notifications text;
   - event severity level.

Note: We recommend you to extract large export files with the WinRAR program. An export file may be incorrectly extracted if you use standard OS tools.

Exporting Unprocessed Host Parameters

You may export monitored hosts' parameters before they are processed by the processing rules. Export is a process of saving the hosts' parameters collected by Monitoring Server into an XML file. You can specify the time interval for which you want to save unprocessed host parameters.

Warning: Exported parameters can be then imported to Microsoft Office Excel or Open Office Calc. To import monitoring events to a program, you must take into account the specifications and limitations of this program.

You can't export unprocessed parameters of the cascaded hosts.

Unprocessed parameters exporting is performed by the Monitoring Server program in the background, so it is possible to work with the monitoring system at the same time.

Note: When you are exporting unprocessed parameters that have been collected over a long period of time or when you are exporting too many host parameters, the exporting process may take time. In this case, the export results are saved at the end of a monitoring session. And when you start a new session, you receive export results of the previous session.

There are two ways you can export the unprocessed host parameters:

- Automatic export. The parameters of automatic export are specified by the Monitoring Server administrator.

  When you schedule the automatic export, it starts in the background with the frequency specified in the Monitoring Server program (by default every 1 hour). The automatic export results are saved to a folder, which you can also specify in the Monitoring Server program. You can enable or disable an automatic export process (by default, this process is disabled).

- Manual export is available both for administrators and for MWA users.

To export unprocessed parameters manually:

1. On the main page, on the **Monitor** tab, click **Export**.
2. In the displayed window:

- Specify the time interval for which you want to save unprocessed host parameters.

> **Note:** If in the specified time interval hosts have been polled several times, then all parameters (including those that changed after polling) will be saved in the export file.

- Choose hosts with the parameters you want to export.

  Select the check boxes of these hosts with the parameters you want to export. To select or unselect all the hosts in the list, use the **All** check box.

  To choose a host from a list, click the icon ⊞ and select the corresponding check box.

  You can also filter hosts by name. To do this, in the search box above the host list, type name or a part of a name. Every time you type a symbol, automatic list filtering is performed according to the occurrence of the typed substring in a host name. To clear the box, click ✕.

3 Click **Export**.

An exporting process will start. During this process, in the notification pane, the icon will be displayed. When the exporting process will be finished, the icon will be displayed.

4 Click . The dialog box prompting you whether an export file should be saved will be displayed. In the request window, click **OK**.

If you export over 60,000 entries, you will be prompted that the created file can't be opened with Microsoft Office Excel.

> **Note:** Each entry contains unprocessed parameters of one host that have been obtained as a query result in the specified time period. For the export file to be available for opening with Microsoft Office Excel, you should decrease the entries number to 60,000. To do this, narrow the events filtering criteria or decrease the number of hosts whose parameters you want to export.

Export of unprocessed hosts parameters has been completed
The export file you have generated contains more than 60 000 rows and cannot be opened in Excel. To create a file to be opened in Excel, decrease the time range.
Save the file 23-09-2014_24-09-2014_ExportTime_17-00-21.zip?
Yes
No

Figure 32: Saving an export file

5 The resulting file will be saved as an archive (a file with a `.zip` extension):

This archive contains an `XML` file with an XML scheme of the selected hosts' parameters (see Structure of the Unprocessed Host Parameters Export File on page 78).

Note: We recommend you to extract large export files with the WinRAR program. An export file may be incorrectly extracted if you use standard OS tools.

Working with Notifications

In Monitoring Web Access, you can see notifications that are formed on the monitoring server when events are registered (see Monitoring event on page 123). The event severity level is defined in each rule.

ViPNet StateWatcher supports various notification types, such as highlighting hosts in a host list, displaying messages, giving sound notifications, sending ViPNet Business Mail, email, and SMS messages. Notifications of a certain type are used only if they are enabled. Only an administrator can enable and disable notifications of certain types when setting the Monitoring Server program. Displaying notifications as well as sending messages to users is performed according to the special notification filters' settings.

Notification filters limit the amount of notifications that a user receives when processing rules are executed. In individual filters for each user it is specified on which hosts an event should be registered to send a notification to this user. Also, you may specify an event severity threshold. Notifications about the events with a severity level equal or higher than the threshold level will be sent to the user. Only an administrator can configure notification filters.

The processing rules specified in the Monitoring Server program are executed every time the hosts are polled. If during a poll a rule is executed, then the notifications are sent in the following order:

- Visual and sound notifications, ViPNet Business Mail, email, and SMS messages are displayed or sent only when an event is registered for the first time. If during the next polls the same change or event is registered, then this notification will not be repeated.
- A host's name is highlighted in the host list or on a map, when an event is registered regardless of previous poll results. The hosts are highlighted till the events on them are fixed.

Visual notifications in the Host List

This notification type is intended for host highlighting on the **Monitor** page.

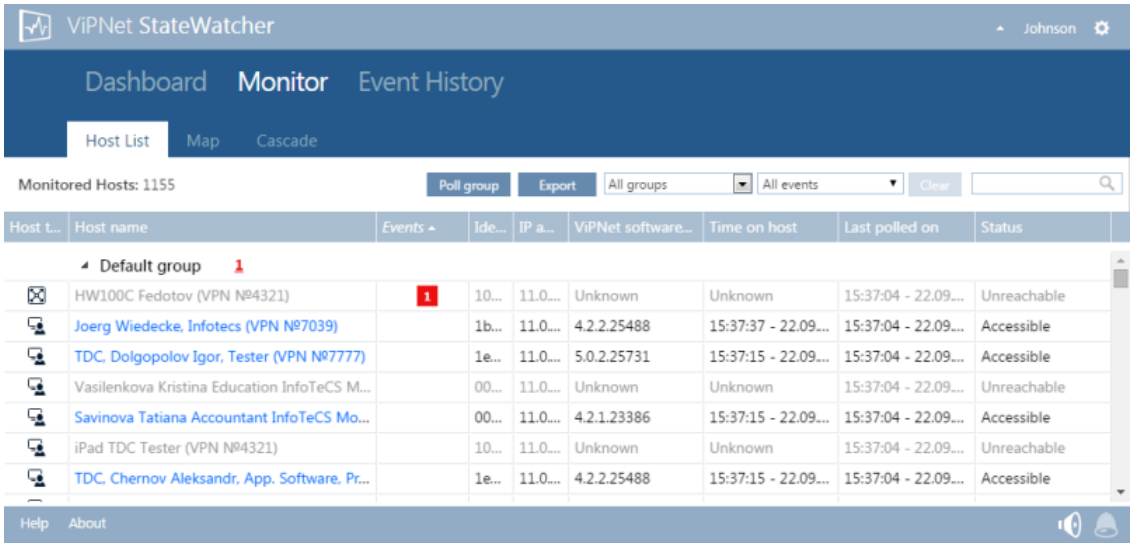
ViPNet StateWatcher
Johnson
Dashboard
Monitor
Event History
Host List
Map
Cascade
Monitored Hosts: 1155
Poll group
Export
All groups
All events
Clear
Host t...
Host name
Events
Ide...
IP a...
ViPNet software...
Time on host
Last polled on
Status
Default group 1
HW100C Fedotov (VPN №4321) 1 10... 11.0.... Unknown Unknown 15:37:04 - 22.09.... Unreachable
Joerg Wiedecke, Infotecs (VPN №7039) 1b... 11.0.... 4.2.2.25488 15:37:37 - 22.09.... 15:37:04 - 22.09.... Accessible
TDC, Dolgopolov Igor, Tester (VPN №7777) 1e... 11.0.... 5.0.2.25731 15:37:15 - 22.09.... 15:37:04 - 22.09.... Accessible
Vasilenkova Kristina Education InfoTeCS M... 00... 11.0.... Unknown Unknown 15:37:04 - 22.09.... Unreachable
Savinova Tatiana Accountant InfoTeCS Mo... 00... 11.0.... 4.2.1.23386 15:37:15 - 22.09.... 15:37:04 - 22.09.... Accessible
iPad TDC Tester (VPN №4321) 10... 11.0.... Unknown Unknown 15:37:04 - 22.09.... Unreachable
TDC, Chernov Aleksandr, App. Software, Pr... 1e... 11.0.... 4.2.2.25488 15:37:15 - 22.09.... 15:37:04 - 22.09.... Accessible
Help
About

Figure 33: Notifications in the host list

If a processing rule for a host is executed, then the icon is displayed in the **Events** column (for example, 1) indicating the number of events registered on this host. The color of this icon corresponds to the event with the highest severity level and is specified by the Monitoring Server administrator.

If there are no icons in this column, it means that there are no events on the host. However, keep in mind that the event icon absence may be caused by this notification type being disabled, the processing rule being edited or deleted, or notifications with the specified severity level being blocked (according to notification filters specified for each user).

Pop-up Messages

Pop-up messages inform you about events registered on hosts, which are displayed on every page of the monitoring system. A notification about a specified event on a host is displayed only when this event is registered for the first time. If during the next poll of this host the same event is found, then it is not repeated. Messages are displayed as windows with detailed or brief event information. There are two pop-up message types:

- Messages in a pop-up window, which are displayed in lower right-hand corner of a page when an event on a monitored host is registered.

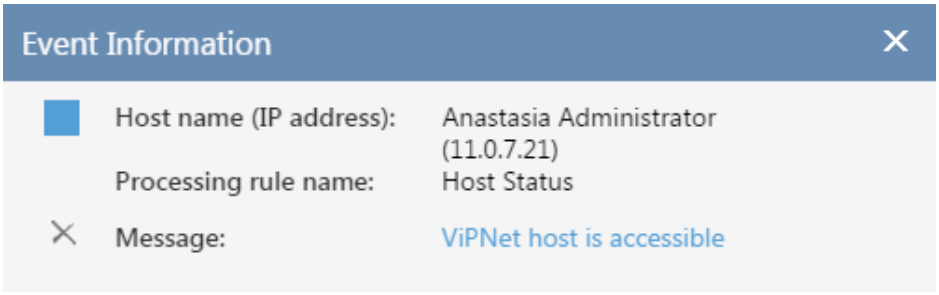

Figure 34: Pop-up message

Messages in pop-up windows include brief event information:

- **Host name (IP address)**, a monitored ViPNet host name and its IP address.
- **Processing rule name**, a rule name.
- **Message**, a message from the Monitoring Server program about the registered event.

By default, messages about the last registered event with the highest severity level are displayed first on the list. If there are more events registered at the same poll, then the 3 last messages with the highest severity level are displayed. Each message is displayed for 3 seconds.

For example, if 50 events occur on one or more hosts (if all messages are enabled for all severity levels), then 3 messages about the events with the highest severity level will be displayed one after another. If there are only 2 events with a critical severity level, then the third message will contain information about an event with the next lower security level.

If necessary, you can also configure notifications for each severity level (see Configuring Pop-up Notifications on page 63).

- Messages in the **Information about events registered on hosts** window. Notifications are displayed in a separate window. Messages about events are displayed just after these events have been registered.

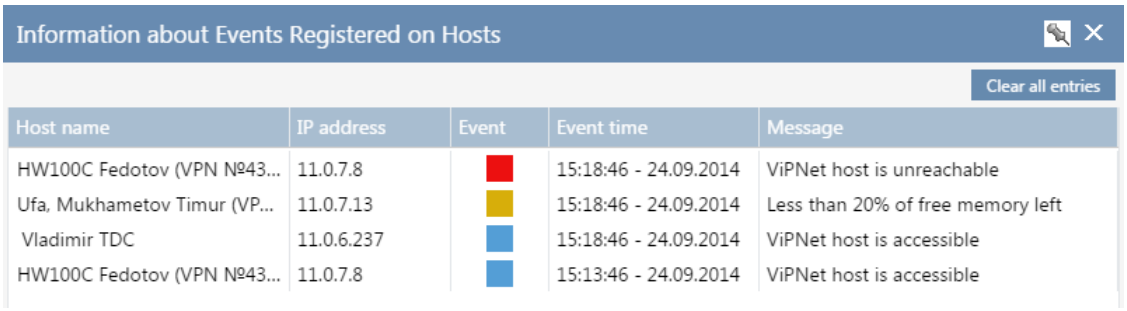

Figure 35: Message in the "Information about events registered on hosts" window

Information about events is shown in a table, where:

- **Host name**, a name of the host where an event has occurred.

- **IP address**, an IP address of the host where an event has occurred.
- **Event**, an event's severity level. The correspondence of a color and a severity level is configured by the administrator.
- **Event time**, the time the event took place.
- **Message**, a message from the Monitoring Server program about the registered event.

The maximum number of events in the table is 50. You can force the clearing of the list by clicking **Clear all entries**. As a result, all event entries will be removed only from the **Information about events registered on hosts** window. These entries will remain in the Monitoring Server log and database, and they will be available when you make another events history request.

You can also pin the **Information about events registered on hosts** window on your screen by clicking . The pinned window will be always displayed on top, so you will be able to work with other features and to view the registered events in the window at the same time. Next time you click the icon , the window will be opened at the place it was positioned during the current Monitoring Server session.

Configuring Pop-up Notifications

On the main page of Monitoring Web Access, you can configure notifications that will be displayed in a pop-up window displaying information about the events of a certain severity level. By default, the notifications for all severity levels are displayed.

To configure notification in a pop-up window only for the required severity level:

1. On the main page of Monitoring Web Access, in the upper-right corner, on the **Settings** menu, click **Configure popup window**.
2. In the **Configure Event Notifications** window, select the **Show notification in a pop-up window** check box. If you don't select this check box, you can view the events by clicking .

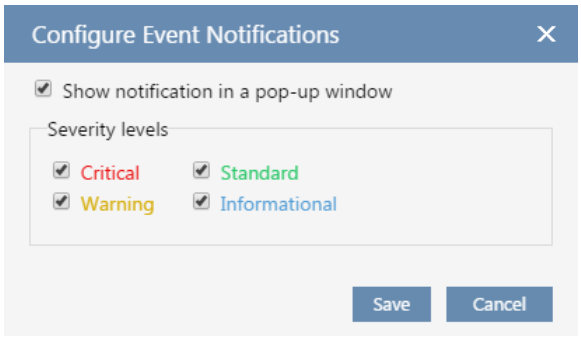

Figure 36: Configuring event notification

3 Under **Severity levels**, select the corresponding check boxes to receive messages about the events with these severity levels.

4 Click **Save**. As a result, in the lower-right corner of the window, messages about events with the chosen severity levels will be displayed in a pop-up window.

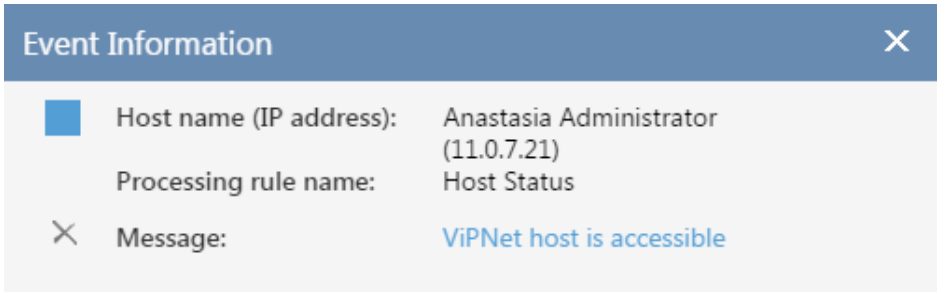

Figure 37: Viewing the pop-up messages

By clicking this pop-up message, you can open the **Host Information** window (see Viewing Information about a Monitored Host on page 32).

Visual notification on the Map

This notification type is implemented by way of the hosts blinking on the map when the processing rules are executed (see Monitoring Hosts on a Map on page 45). The blinking color corresponds to the event of the highest severity level among the events detected. If there is no blinking, then no events are detected on the host. However, keep in mind that no blinking may be caused by this notification type being disabled, the processing rule being edited or deleted, or notifications with the specified severity level being blocked (according to notification filters specified for each user).

You can disable notification for a monitored host on its monitoring server. In such a case, there will be no blinking, even though some events are detected after processing rules execution. Notification will be enabled when the specified time expires or on user's request.

Cascaded hosts may fail to blink if, at some point in a cascade, the connection is broken, for example, if some child monitoring servers are switched off.

Sound Notifications

Sound notifications are played in Monitoring Web Access when an event is registered on a host. Each severity level has its own sound file (with an `.mp3` extension). These connections are specified by the administrator during the Monitoring Server configuring.

Sound notification about an event on a host is played only when it is registered for the first time. If during the next poll the same event is found on the host, the sound notification is not repeated. If several processing rules are executed at the same time, the sound file of the maximum severity level established by the executed rules is played.

Email Notifications

Email notifications are the notifications that are sent to monitoring server's users when processing rules are executed. Messages are sent to the email addresses specified in the user accounts. A message about an event is sent to a host only when this event is registered for the first time. If during the next poll the same event is found on this host, then the email message about it is not sent again.

The email message subject has the following text: “Processing rule notification <processing rule name> on the host <host name>, <host IP address>”. The message text is formed according to the template specified by the administrator during the Monitoring Server configuring.

According to the template from the ViPNet StateWatcher monitoring system distribution kit, the message body consists of the following data:

- processing rule name;
- processing rule severity level;
- monitored host name;
- monitored ViPNet host identifier;
- monitoring server name;
- time and date of a processing rule execution;
- message text about a host status change or about a critical event.

ViPNet Business Mail Notifications

ViPNet Business Mail (on page 125) notifications are text files (messages) that are sent to the users after a processing rule execution by using the ViPNet Business Mail program. A message about a status change or about a host event is sent only once when this change or event is registered for the first time. If during the next poll the same status change or critical event was registered on the same host, the message is not sent again via ViPNet Business Mail.

The file includes message text about a host status change or about a critical event. The file name is formed according to the following template: `<host name>_<host identifier>_<rule name>_<execution time>.txt`.

Note: The file with a text is attached to the incoming email message. The length of the attachment name has limitations, which is why the attachment name may be a shortened file name. At the same time, the file name remains unchanged and is fully displayed after you save the attachment on your hard drive.

According to ViPNet Business Mail autoprocessing rules, the files are sent to the ViPNet hosts' users who monitor hosts via Monitoring Web Access. The messages transferred from a monitoring server to a MWA host are saved to the `Inbox` folder. When the messages are being received, the ViPNet Business Mail program notifies the users about it.

SMS Notifications

SMS notifications are SMS messages automatically created based on the corresponding processing rule's message and some service information. The standard length of an SMS message is 70 characters. If the notification text is longer than that, the notification is divided into several SMS notifications, no longer than 70 characters each. Every SMS notification includes several fields containing the following information:

- the Monitoring Server's name (maximum 40 characters);
- the processing rule's name (maximum 40 characters);
- the monitoring event's severity level (maximum 10 characters);
- the name of the host where the processing rule was applied (maximum 40 characters);
- the time when the processing rule is applied;
- the processing rule's message text (maximum 70 characters).

The length of each is limited. If any field exceeds this limit, the full text won't be displayed in the SMS notification.

SMS notifications are sent to the users' phone numbers. The Monitoring Server administrator specifies these phone numbers in the accounts of the users who should receive such notifications by SMS.

Statistics

One of the main tasks that the Monitoring Server program solves is gathering statistics about the ViPNet hosts. The collected data is displayed on the **Monitor > Cascade** page. On this tab, the statistics is displayed both for the hosts managed directly and for the cascaded hosts. The tab includes data about the quantity of the events with different severity levels registered on the monitored hosts. The data is shown in the statistics table depending on the category of the host where an event was registered. On the statistics page, the hosts are divided into the two categories: cascaded hosts and hosts monitored directly. On the statistics page, you may also view the total number of events with a specific severity level as well as host statuses regardless of their categories.

In Monitoring Web Access, you can view both the cascade statistics (for the cascade parts you have access to), and the structure of the cascade parts.

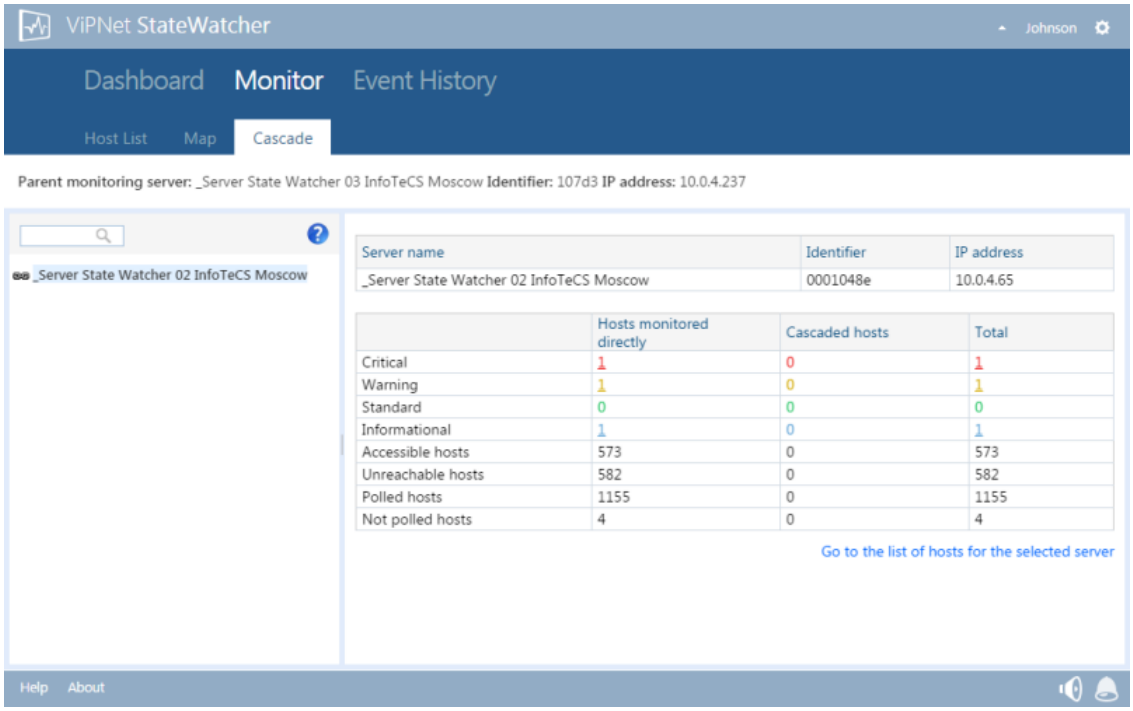

Figure 38: Viewing the statistics and the cascade structure

With the data on the statistics page you can assess the monitoring server work and define the critical areas of your network.

Viewing the Statistics for a Cascade Segment

To view statistics for the specific cascade segment:

1. On the **Monitor** tab, click **Cascade**.
2. In the navigation pane, choose the monitoring server whose statistics you want to see.

   If necessary, expand the monitoring servers list by clicking the icon ⊞, which you can find to the left of a server name.

   You can also filter monitoring servers by name. To do this, type the name or a part of the name in the search box above the server list. Every time you type a symbol, the automatic list filtering is performed according to the occurrence of the typed symbols in a server name. To clear the box, click ✕.

Warning: Statistics is displayed only for monitoring servers, which are connected in a cascade and are accessible.

Table 6: Servers status displaying in MWA

Server icon	Description
	Cascade relation has been established
	Cascade relation has not been established
	Waiting for the cascade relation to be established or broken

3. In the view pane, two tables will be displayed:
   - General information table. This table includes the following parameters:
     - **Server name** is the name of a server, the statistics of which you are viewing.
     - **Identifier** is an identifier of a network server.
     - **IP address** is an IP address of a server on the network.
   - Statistics table. The table includes information about quantity and statuses of monitored hosts.

     There are 3 categories of the monitored hosts in the table:

     - **Hosts monitored directly** are hosts that are monitored by this server. In the statistics of directly monitored hosts all hosts where the events with the specified severity level were registered are taken in account.

- **Cascaded hosts** are hosts that are monitored by one of your child monitoring servers.
- **Sum** is the total number of hosts regardless of the way they are monitored.

The color and number of a table entry depends on the following parameters:

- **Critical** is the number of hosts on which critical events were registered. The number of hosts is red.
- **Warning** is the number of hosts on which the events with warning severity level were registered. The number of hosts is yellow.
- **Standard** is the number of hosts on which the least critical events were registered. The number of hosts is green.
- **Informational** is the number of hosts on which the events of informational type were registered. The number of hosts is blue.
- **Accessible hosts** is the number of hosts with the **Accessible** status registered during the poll.
- **Unreachable hosts** is the number of hosts with the **Unreachable** status registered during the poll.
- **Polled hosts** is the number of hosts which are added for monitoring and for which polling is enabled.
- **Not polled hosts** is the number of hosts which are not added for monitoring and also hosts which are added for monitoring but for which polling is disabled.

4 In the cell on the crossing of the required host type and the required severity level click the number that represents the quantity of the events that occurred as a result of processing rules execution.

Note: The number in the cell corresponds to the number of hosts on which events had been registered at the moment of viewing the statistics.

5 As a result, the host list of the **Monitor** page will be opened, where the host list of the monitoring server with chosen host type and events of chosen severity level will be shown.

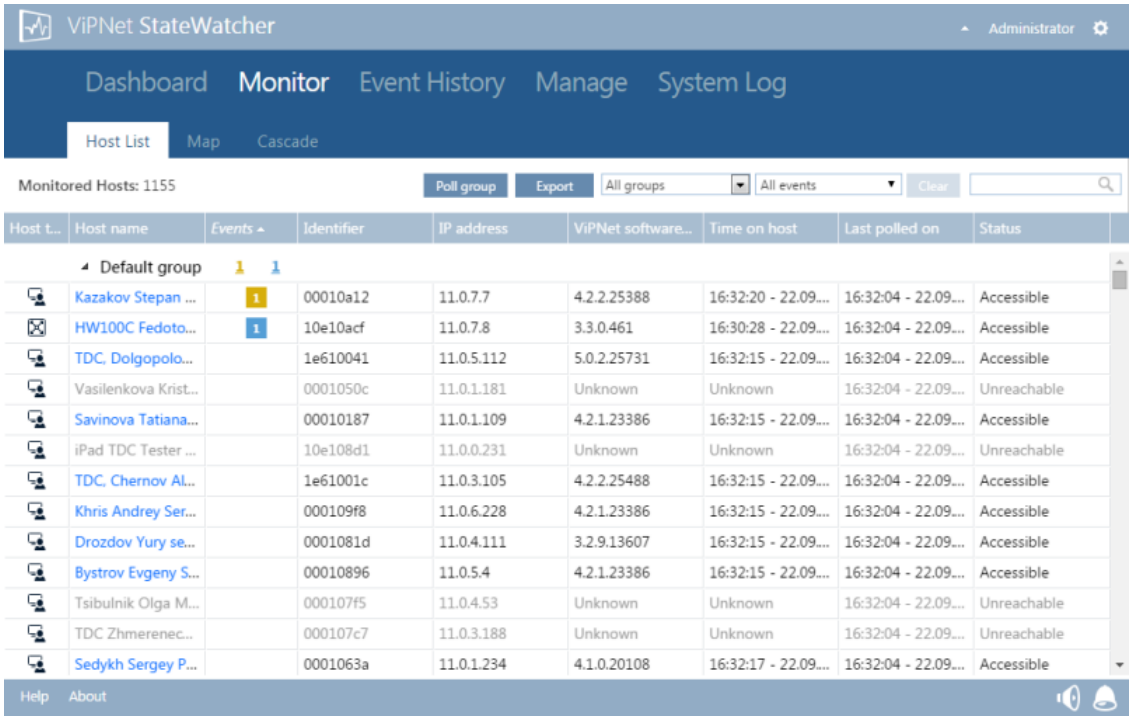

Figure 39: Displaying the events with the chosen severity level

Warning: If for some hosts the notification process was stopped or a notification filter was enabled, after you click the number in a column on the monitoring page, these hosts are not displayed in a list, because if the notification process is not functioned and when there is a notification filter the hosts are removed from the **Monitor** page.

Monitoring the Network Health

With Monitoring Web Access, you can be informed about the state of your ViPNet network hosts real-time. The information is displayed as a graph. The following parameters may be placed along the timescale:

- The number of accessible monitored hosts in the ViPNet network.
- The number of accessible coordinators.
- The number of accessible clients.
- The number of accessible cascaded monitored hosts in the ViPNet network.
- The number of accessible cascaded coordinators.
- The number of accessible cascaded clients.
- The number of events with the **Informational** severity level.
- The number of events with the **Standard** severity level.
- The number of events with the **Warning** severity level.
- The number of events with the **Critical** severity level.
- The number of monitored hosts with the **Informational** severity level in your network.
- The number of monitored hosts with the **Standard** severity level in your network.
- The number of monitored hosts with the **Warning** severity level in your network.
- The number of monitored hosts with the **Critical** severity level in your network.

The network state information can be displayed at the bottom of the main MWA page or in a separate window:

- To display the **Network Health** pane, in the main window, on the **Settings** menu, click **Show Network Health pane**. As a result, the **Network Health** pane will be displayed at the bottom of the main window.

Figure 40: Show the Network Health pane

- To display the network status information in a separate window, click .
- To hide the **Network Health** pane, click or, on the **Settings** menu, click **Hide Network Health pane**.

For the **Network Health** pane, see the following figure.

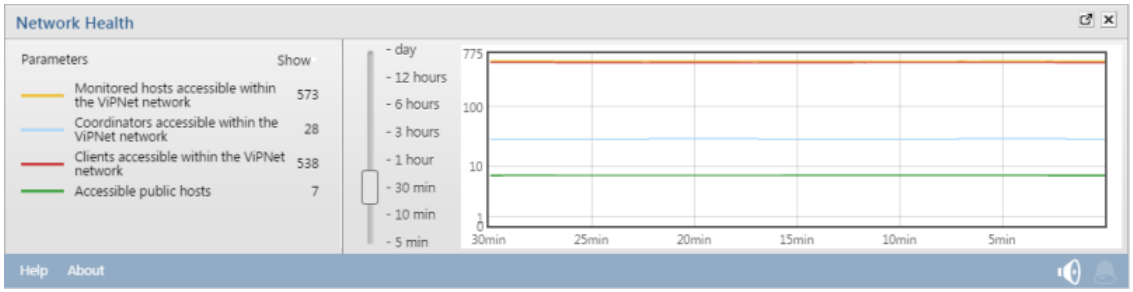

Figure 41: Network health information

In the right part of the pane, the network state graph is displayed along the timescale. The parameters on the graph are refreshed every five seconds. The older values are shifted left respectively to the timescale.

The passed time is displayed on the timescale, from right to left. Thus, at the most right graph point, the new parameter values are displayed, while the values received, for example, 30 minutes ago are displayed at the most left graph point. To choose the necessary time scale from 5 minutes to a day, move the slider bar up or down.

In the left part of the pane, the parameters added to the graph earlier are displayed. To add or remove a graph parameter, click **Show** and select or clear the corresponding check boxes.

Troubleshooting

Here you will find a list of possible Monitoring Web Access malfunctions and the corresponding troubleshooting guidelines.

Can't Connect to the Monitoring Server via a Web Browser

Description:

- You can't connect to the Monitoring Server program via a web browser, and you don't see the logon window.

Cause and solution:

- The Apache Tomcat service is not running on the monitoring server.

  Inform your administrator about the problem. Find out the reason the service was stopped and ask the administrator to start Apache Tomcat.

- The monitored host is not connected with the monitoring server.

  Check the connection between the host and your monitoring server in the ViPNet Client Monitor program or by executing the `ping` command. If there is no connection, ask your administrator to check that host links are properly set in the ViPNet Network Manager program.

Possible Malfunctions

Description:

- At the web application startup or during its operation, you are notified that the “Monitoring server” role is not assigned to the server host.

Cause and solution:

- The Monitoring Server program has been stopped because of the licensing terms violation.

  Inform the administrator of the Monitoring Server program or your ViPNet network administrator about the problem and ask him or her to check whether the “Monitoring server” role is assigned to the server host.

Description:

- At the web application startup or during its operation, you are notified that the permitted number of monitored hosts has been exceeded.

Cause and solution:

- The Monitoring Server program has been stopped because of the violation of the licensing terms related to the limitation on the monitored hosts number.

  Inform the administrator of the Monitoring Server program or your ViPNet network administrator about the problem. Ask the administrator to modify the limitation (to increase the allowed number of monitored hosts) in the ViPNet Network Manager program or to remove unnecessary hosts from the list of monitored hosts.

Description:

- When you are browsing a web application's page (you are clicking a button or a link, a log entry, and so on), you are notified that the monitoring server is inaccessible.

Cause and solution:

- The Monitoring Server program has been stopped.

  Inform your administrator about the problem. Find out why the program was stopped and ask him or her to start the Apache Tomcat service. After you start the Apache Tomcat service, the Monitoring Server program starts automatically.

Description:

- When you are browsing a web page (clicking a button or a link, a log entry, and so on), the user logon window is displayed.

Cause and solution:

- The Monitoring Server program has been restarted, and Monitoring Web Access has reconnected to the monitoring server.

  To access the monitoring server again, enter your user name and password.

Too Many Monitored Hosts.

Description:

- At the web application startup or during its operation, you are notified that the permitted number of monitored hosts has been exceeded.

Cause and solution:

- The Monitoring Server program has been stopped because of the violation of the licensing terms related to the limitation on the monitored hosts number.

  Inform the administrator of the Monitoring Server program or your ViPNet network administrator about the problem. Ask the administrator to modify the limitation (to increase the allowed number of monitored hosts) in the ViPNet Network Control Center program or to remove unnecessary hosts from the list of monitored hosts.

Monitoring Server is Unavailable

Description:

- When you are browsing a web application's page (you are clicking a button or a link, a log entry, and so on), you are notified that the monitoring server is inaccessible.

Cause and solution:

- The Monitoring Server program has been stopped.

Inform your administrator about the problem. Find out why the program was stopped and ask him or her to start the Apache Tomcat service. After you start the Apache Tomcat service, the Monitoring Server program starts automatically.

StateWatcher Role Is Not Registered

Description:

- At the web application startup or during its operation, you are notified that the "StateWatcher" role is not assigned to the server host.

Cause and solution:

- The Monitoring Server program has been stopped because of the licensing terms violation.

  Inform the administrator of the Monitoring Server program or your ViPNet network administrator about the problem and ask him or her to check whether the "StateWatcher" role is assigned to the server host.

Cannot Open a Host Details Window

Description:

- You work in Internet Explorer version 9.0. On the **Monitor** > **Host List** page, you click the link with the monitored host name, but the host information window will not open.

Cause and solution:

- To solve this problem, we recommend you to update Internet Explorer to version 10.0.
- If you do not want to update your browser, change security settings of your Internet Explorer 9.0:

  5.1 Open Internet Explorer.

  5.2 Click **Tools** , and then click **Internet options**.

  5.3 On the **Security** tab, select the **Internet** zone icon, and then click **Custom level**.

  5.4 On the **Settings** list, navigate to **Scripting** > **Active scripting**.

  5.5 Select **Enable**, click **OK**, and then click **OK** once again.

Need to Re-Authenticate the User

Description:

- When you are browsing a web page (clicking a button or a link, a log entry, and so on), the user logon window is displayed.

Cause and solution:

- The Monitoring Server program has been restarted, and Monitoring Web Access has reconnected to the monitoring server.

  To access the monitoring server again, enter your user name and password.

Problems During Unprocessed Host Parameters Exporting

Description:

- If an error occurred during unprocessed host parameters exporting, in the notification pane, in the lower right-hand corner, the icon will be displayed. To view the export error, click the icon . A window with an error text will be displayed.

Cause and solution:

- An error occurred while creating an XML file. To solve this problem, try to start the export process again.
- The hard disk where the export file is being uploaded is full. To solve this problem, free up necessary disk space and try to start the export process again.
- The customization pack updating process started while an exported file was being uploaded. To solve this problem, stop the customization pack updating process and wait until the export process finishes.
- Unexpected error. To solve this problem, try to start the export process again.

B

Structure of the Unprocessed Host Parameters Export File

This appendix displays the XML scheme according to which the export of unprocessed host parameters is performed. When an export file is being created, the UTF-8 encoding is used.

```
<?xml version=1.0 encoding=utf-8?>
<xs:schema attributeFormDefault=unqualified elementFormDefault=qualified
xmlns:xs=http://www.w3.org/2001/XMLSchema>
  <xs:element name=export type=exportType/>
  <xs:complexType name=ifaceType>
    <xs:sequence>
      <xs:element type=xs:string name=iface-id/>
      <xs:element type=xs:string name=iface-name/>
      <xs:element type=xs:string name=iface-ip/>
      <xs:element type=xs:string name=iface-netmask/>
      <xs:element type=xs:string name=iface-mode/>
      <xs:element type=xs:string name=iface-start-mode/>
      <xs:element type=xs:string name=iface-ext/>
      <xs:element type=xs:string name=iface-used/>
      <xs:element type=xs:string name=iface-timediff/>
      <xs:element type=xs:string name=iface-max-log-size/>
      <xs:element type=xs:string name=iface-reg-all/>
      <xs:element type=xs:string name=iface-reg-broadcast/>
      <xs:element type=xs:string name=iface-reg-tcp-serv-port/>
      <xs:element type=xs:string name=enc-in-pass/>
```

```
      <xs:element type=xs:string name=enc-out-pass/>
      <xs:element type=xs:string name=enc-in-drop/>
      <xs:element type=xs:string name=enc-out-drop/>
      <xs:element type=xs:string name=unenc-in-pass/>
      <xs:element type=xs:string name=unenc-out-pass/>
      <xs:element type=xs:string name=unenc-in-drop/>
      <xs:element type=xs:string name=unenc-out-drop/>
      <xs:element type=xs:string name=enc-in-br-pass/>
      <xs:element type=xs:string name=enc-out-br-pass/>
      <xs:element type=xs:string name=enc-in-br-drop/>
      <xs:element type=xs:string name=enc-out-br-drop/>
      <xs:element type=xs:string name=unenc-in-br-pass/>
      <xs:element type=xs:string name=unenc-out-br-pass/>
      <xs:element type=xs:string name=unenc-in-br-drop/>
      <xs:element type=xs:string name=unenc-out-br-drop/>
      <xs:element type=xs:string name=enc-in-pass-bytes/>
      <xs:element type=xs:string name=enc-out-pass-bytes/>
      <xs:element type=xs:string name=enc-in-drop-bytes/>
      <xs:element type=xs:string name=enc-out-drop-bytes/>
      <xs:element type=xs:string name=unenc-in-pass-bytes/>
      <xs:element type=xs:string name=unenc-out-pass-bytes/>
      <xs:element type=xs:string name=unenc-in-drop-bytes/>
      <xs:element type=xs:string name=unenc-out-drop-bytes/>
      <xs:element type=xs:string name=enc-in-br-pass-bytes/>
      <xs:element type=xs:string name=enc-out-br-pass-bytes/>
      <xs:element type=xs:string name=enc-in-br-drop-bytes/>
      <xs:element type=xs:string name=enc-out-br-drop-bytes/>
      <xs:element type=xs:string name=unenc-in-br-pass-bytes/>
      <xs:element type=xs:string name=unenc-out-br-pass-bytes/>
      <xs:element type=xs:string name=unenc-in-br-drop-bytes/>
      <xs:element type=xs:string name=unenc-out-br-drop-bytes/>
      <xs:element type=xs:string name=traffic-total-in/>
      <xs:element type=xs:string name=traffic-total-out/>
      <xs:element type=xs:string name=traffic-total/>
      <xs:element type=xs:string name=traffic-load/>
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name=tunnelsType>
    <xs:sequence>
      <xs:element type=tunnelType name=tunnel maxOccurs=unbounded
      minOccurs=0/>
    </xs:sequence>
  </xs:complexType>
```

```
<xs:complexType name=exportType>
  <xs:sequence>
    <xs:element type=recordType name=record/>
  </xs:sequence>
</xs:complexType>
<xs:complexType name=tunnelType>
  <xs:sequence>
    <xs:element type=xs:string name=start-address/>
    <xs:element type=xs:string name=end-address/>
  </xs:sequence>
</xs:complexType>
<xs:complexType name=diskType>
  <xs:sequence>
    <xs:element type=xs:string name=disk-name/>
    <xs:element type=xs:string name=device/>
    <xs:element type=xs:string name=capacity/>
    <xs:element type=xs:string name=free-space/>
    <xs:element type=xs:string name=disk-usage-int/>
  </xs:sequence>
</xs:complexType>
<xs:complexType name=ifacesType>
  <xs:sequence>
    <xs:element type=ifaceType name=iface maxOccurs=unbounded minOccurs=0/>
  </xs:sequence>
</xs:complexType>
<xs:complexType name=eventType>
  <xs:sequence>
    <xs:element type=xs:string name=event-type/>
    <xs:element type=xs:string name=event-timestamp/>
    <xs:element type=xs:string name=event-source/>
    <xs:element type=xs:string name=event-category/>
    <xs:element type=xs:string name=user/>
    <xs:element type=xs:string name=event-node/>
    <xs:element type=xs:string name=event-description/>
    <xs:element type=xs:string name=journal/>
  </xs:sequence>
</xs:complexType>
<xs:complexType name=recordType>
  <xs:sequence>
    <xs:element type=xs:string name=node-id/>
    <xs:element type=xs:string name=monitor-status/>
    <xs:element type=xs:string name=node-status/>
    <xs:element type=xs:string name=node-name/>
```

```
      <xs:element type=xs:string name=node-type/>
      <xs:element type=xs:string name=node-timestamp/>
      <xs:element type=xs:string name=product-version/>
      <xs:element type=xs:string name=drv-version/>
      <xs:element type=xs:string name=monitor-version/>
      <xs:element type=xs:string name=pkt-log-version/>
      <xs:element type=xs:string name=pkt-type/>
      <xs:element type=xs:string name=server-id/>
      <xs:element type=xs:string name=is-server/>
      <xs:element type=xs:string name=ip-list/>
      <xs:element type=xs:string name=server-poll-timeout/>
      <xs:element type=xs:string name=dudp/>
      <xs:element type=xs:string name=dudp-always-use-server/>
      <xs:element type=xs:string name=virtual-ip/>
      <xs:element type=xs:string name=firewall-ip/>
      <xs:element type=xs:string name=proxy-id/>
      <xs:element type=xs:string name=port/>
      <xs:element type=xs:string name=use-firewall/>
      <xs:element type=xs:string name=firewall-type/>
      <xs:element type=xs:string name=fix-firewall/>
      <xs:element type=xs:string name=task-list/>
      <xs:element type=xs:string name=forward-id/>
      <xs:element type=ifacesType name=ifaces/>
      <xs:element type=disksType name=disks/>
      <xs:element type=xs:string name=cpu-usage/>
      <xs:element type=xs:string name=memory-total/>
      <xs:element type=xs:string name=memory-free/>
      <xs:element type=xs:string name=memory-usage/>
      <xs:element type=xs:string name=disk-usage_int/>
      <xs:element type=xs:string name=mftp-status/>
      <xs:element type=xs:string name=mftp-queue-length/>
      <xs:element type=xs:string name=mftp-queue-size/>
      <xs:element type=tunnelsType name=tunnels/>
      <xs:element type=xs:string name=bmail-status/>
      <xs:element type=xs:string name=failover-status/>
      <xs:element type=eventsType name=events/>
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name=disksType>
    <xs:sequence>
      <xs:element type=diskType name=disk maxOccurs=unbounded minOccurs=0/>
    </xs:sequence>
  </xs:complexType>
```

```
  <xs:complexType name=eventsType>
    <xs:sequence>
      <xs:element type=eventType name=event maxOccurs=unbounded minOccurs=0/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

When you view an export file as a table, the names of the elements specified in the XML scheme are displayed as column headers. The correspondence between the element names and the parameters being exported is shown in the table below.

Table 7: The correspondence between the scheme elements and the parameters being exported

Element name	Parameter being exported
poll-timestamp	The last date and time when the host was polled by the Monitoring Server program.
node-id	ViPNet host identifier
monitor-status	ViPNet Monitor program's status
node-status	Host status
node-name	Host name
node-type	Host type
node-timestamp	The current time and date on the monitored host
product-version	ViPNet software version
drv-version	ViPNet driver version
monitor-version	ViPNet control daemon version
pkt-log-version	IP packets log version
pkt-type	Encrypted packets format
server-id	VPN server identifier for a host
is-server	ViPNet server flag
ip-list	List of host's IP addresses
server-poll-timeout	External ViPNet server polling period in the dynamic UDP mode
dudp	Dynamic UDP flag
dudp-always-use-server	External ViPNet server in the dynamic UDP mode flag
virtual-ip	Host virtual address
firewall-ip	Firewall IP address
proxy-id	Proxy server identifier

Element name	Parameter being exported
poll-timestamp	The last date and time when the host was polled by the Monitoring Server program.
port	Firewall port for UDP packets
use-firewall	Firewall flag
firewall-type	Firewall type
fix-firewall	Fixed firewall settings flag
task-list	Host roles list
forward-id	Identifier of a VPN server used in the dynamic UDP mode
iface-id	Interface identifier
iface-name	Interface name
iface-ip	List of network interface IP addresses
iface-netmask	Network interface subnet mask
iface-mode	Current interface security level
iface-start-mode	Start interface security level
iface-ext	External interface flag
iface-used	Interface usage flag
iface-timediff	IP packets registration log entries aggregation period
iface-max-log-size	Maximum IP packets log size
iface-reg-all	All IP packets logging flag
iface-reg-broadcast	Broadcast IP packets logging flag
iface-reg-tcp-serv-port	Server port for TCP packets logging flag
enc-in-pass	The number of successfully received encrypted IP packets
enc-out-pass	The number of allowed outgoing encrypted IP packets
enc-in-drop	The number of blocked incoming encrypted IP packets
enc-out-drop	The number of blocked outgoing encrypted IP packets
unenc-in-pass	The number of allowed incoming non-encrypted IP packets
unenc-out-pass	The number of successfully sent non-encrypted IP packets
unenc-in-drop	The number of blocked incoming non-encrypted IP packets
unenc-out-drop	The number of blocked outgoing non-encrypted IP packets
enc-in-br-pass	The number of allowed incoming encrypted broadcast IP packets
enc-out-br-pass	The number of allowed outgoing encrypted broadcast IP packets

Element name	Parameter being exported
poll-timestamp	The last date and time when the host was polled by the Monitoring Server program.
enc-in-br-drop	The number of blocked incoming encrypted broadcast IP packets
enc-out-br-drop	The number of blocked outgoing encrypted broadcast IP packets
unenc-in-br-pass	The number of allowed incoming non-encrypted broadcast IP packets
unenc-out-br-pass	The number of allowed outgoing non-encrypted broadcast IP packets
unenc-in-br-drop	The number of blocked incoming non-encrypted broadcast IP packets
unenc-out-br-drop	The number of blocked outgoing non-encrypted broadcast IP packets
enc-in-pass-bytes enc-out-pass-bytes enc-in-drop-bytes enc-out-drop-bytes unenc-in-pass-bytes unenc-out-pass-bytes unenc-in-drop-bytes unenc-out-drop-bytes enc-in-br-pass-bytes enc-out-br-pass-bytes enc-in-br-drop-bytes enc-out-br-drop-bytes unenc-in-br-pass-bytes unenc-out-br-pass-bytes unenc-in-br-drop-bytes unenc-out-br-drop-bytes	Every element with the "-bytes" postfix includes the total size (in MB) of the packets. The number of the packets is displayed in the element with the corresponding name. For example, the **enc-in-pass-bytes** element includes the total size of the packets, the number of which is displayed in the **enc-in-pass** element (that is the total size of successfully received encrypted packets).
traffic-total-in	Total incoming IP traffic
traffic-total-out	Total outgoing IP traffic
traffic-total	Total incoming and outgoing IP traffic
traffic-load	Load on a network interface
disk-name	Disk letter
device	Physical device name
capacity	Total disk space

Element name	Parameter being exported
poll-timestamp	The last date and time when the host was polled by the Monitoring Server program.
free-space	Free disk space
disk-usage	Disk space usage (per cent)
cpu-usage	CPU load (per cent)
memory-total	Total physical memory (RAM)
memory-free	Free physical memory (RAM)
memory-usage	RAM usage (per cent)
disk-usage-int	Disk space usage (per cent)
mftp-status	MFTP status
mftp-queue-length	The number of envelopes in the queue
mftp-queue-size	Total size of all the envelopes in the queue
start-address	Start IP address of the tunneled addresses range
end-address	End IP address of the tunneled addresses range
bmail-status	ViPNet Business Mail status
failover-status	Failover service status
event-type	Event type
event-timestamp	Date and time of the event
event-source	Event source name
event-category	Event category
user	The name of the user who invoked the event
event-node	ViPNet host on which the event has occurred
event-description	Event description
journal	Log containing the event entry

Structure of the Events History Export File

This appendix displays the XML scheme according to which results of applying processing rules are exported. When an export file is being created, the UTF-8 encoding is used.

```
<?xml version=1.0 encoding=utf-8?>
<xs:schema attributeFormDefault=unqualified elementFormDefault=qualified
xmlns:xs=http://www.w3.org/2001/XMLSchema>
  <xs:element name=results type=resultsType/>
  <xs:complexType name=resultType>
    <xs:sequence>
      <xs:element type=xs:string name=node-id/>
      <xs:element type=xs:string name=node-name/>
      <xs:element type=xs: timestamp name=event-start-timestamp/>
      <xs:element type=xs:timestamp name=event-end-timestamp/>
      <xs:element type=xs:string name=rule-id/>
      <xs:element type=xs:string name=rule-name/>
      <xs:element type=xs:string name=rule-node-id/>
      <xs:element type=xs:string name=severity/>
      <xs:element type=xs:string name=message/>
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name=resultsType>
    <xs:sequence>
```

```
      <xs:element type=resultType name=result maxOccurs=unbounded
      minOccurs=0/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

When you view an export file as a table, the names of the elements specified in the XML scheme are displayed as column headers. The correspondence between the element names and the data being exported is shown in the table below.

Table 8: The correspondence between the scheme elements and the data being exported

Element name	Data being exported
node-id	Monitored host identifier
node-name	Monitored host name
event-start-timestamp	Start date and time of the event
event-end-timestamp	End date and time of the event
rule-id	Processing rule identifier
rule-name	Processing rule name
severity	Event severity level
message	Notification text formed by a processing rule

Monitored Parameters

Parameters Monitored on Hosts

In this appendix, you will find a list of parameters that are monitored in the current version of the ViPNet StateWatcher monitoring system. The parameters are joined into the same logical groups as in the Monitoring Web Access. Each logical group of parameters is described in a separate table. For each parameter, you can see its name, format, brief description, type of data, and, if necessary, the possible values.

Some parameters can be controlled only in later versions of the software: for ViPNet Client and ViPNet Coordinator, in 3.1.3 version or later; for ViPNet Coordinator Linux, in 3.6.1 version or later; for the ViPNet Coordinator HW software-hardware appliance, in 2.2 version or later. Such version-dependent parameters are marked with an asterisk (*).

Note: If ViPNet Client or ViPNet Coordinator version earlier than 3.1 or ViPNet Coordinator Linux version earlier than 3.4 is installed on a host, parameters can't be monitored.

If, on a monitored host, ViPNet programs other than ViPNet Client and ViPNet Coordinator are installed, then the state of the program components Business Mail and MFTP will not be monitored. The status of these programs will be **Off-line**.

Table 9: General characteristics of a monitored host

Parameter name	Description	Format	Possible values
ViPNet host identifier	The identifier of the ViPNet host	A hexadecimal number	

Parameter name	Description	Format	Possible values
		For example: **10e11972**	
Name	ViPNet host name	String	
Description	Host description	String	Maximum 1024 bytes
Current time	The current time and date on the monitored host	HH:MM:SS - DD.MM.YYYY For example: **10:54:27 - 02.02.2011**	
Host status	Accessibility of the host on the ViPNet network	String	**Accessible** **Unreachable** **Not defined**
ViPNet host type	Host type on the ViPNet network	String	**Client** **Coordinator** **Not defined**
Host type	Type of the host in the monitoring system	String For example, **Cluster**, **HW1000**	
ViPNet Monitor status	ViPNet Monitor activity on the host	String	**Online** **Offline** **UDB protocol error** **Unknown**

Parameter name	Description	Format	Possible values
			None **Not defined**
Host's VPN server identifier	The identifier of the host's IP addresses server	A hexadecimal number For example: **10e11972**	
Host's VPN server	Whether the host functions as the IP addresses server on the network	String	**Yes** **No** **Not defined**
List of host's IP addresses		A string that consists of an IP address or several IP addresses divided by a comma For example: **10.0.2.230, 192.168.16.1**	
Added roles	A list of roles assigned to the host	A string, which consists of role names divided by a comma For example: **Business Mail,VPN host,Monitoring Client**	
Total physical memory (RAM)*	Measured in megabytes (**MB**)	Integer For example: **4,094 MB**	
Free physical memory (RAM)*	Measured in megabytes (**MB**)	Integer	

Parameter name	Description	Format	Possible values
Memory usage*	RAM usage (**%**)	Integer For example: **66 %**	
CPU load*	CPU load per cent (**%**)	Integer	
Business Mail*	ViPNet Business Mail status	String	**Online** **Offline** **UDB protocol error** **Unknown** **None** **Not defined**
Cluster	Work in the hot failover cluster mode	String	
Failover module status	Failover status on the active cluster node	String	**Online** **Offline** **UDB protocol error** **Unknown** **None** **Not defined**

Table 10: General characteristics of a monitored host: Disks

Parameter name	Description	Format	Possible values
Disk name*	Disk letter	Symbol For example: **D**	
Device name*	Physical device name	String For example: **\Device\HarddiskVolume3**	
Total disk space*	Measured in megabytes (**MB**)	Integer For example: **52,619 MB**	
Free*	Free disk space in megabytes (**MB**)	Integer	
Used*	Disk space usage per cent (**%**)	Integer For example: **18 %**	

Table 11: General characteristics of a monitored host: System events log

Parameter name	Description	Format	Possible values
System log			
Event time*	Date and time of the event	HH:MM:SS - DD.MM.YYYY For example: **10:41:24 - 03.02.2011**	
Event type*		String	

Parameter name	Description	Format	Possible values
		For example: **Information**	
Source*	Event source name	String	
Category*	Event category	String	
User*	The name of the user who invoked the event	String	
Description*	Event description	String	
Application log			
Event time*	Date and time of the event	HH:MM:SS - DD.MM.YYYY	
Event type*		String	
Source*	Event source name	String	
Category*	Event category	String	
User*	The name of the user who invoked the event	String	
Description*	Event description	String	

Table 12: ViPNet Monitor parameters

Parameter name	Description	Format	Possible values
ViPNet Monitor or ViPNet control daemon version	The version of the ViPNet Monitor program or ViPNet control daemon	3 or 4 numbers divided by a period	

Parameter name	Description	Format	Possible values
		For example: **3.1.3.7623**	
Driver version	ViPNet network protection driver version	3 numbers divided by a period For example: **3.0.437**	
IP packets type	The format of outgoing encrypted packets addressed to ViPNet hosts	2 numbers divided by a period	**4.0** **4.1**
Host type	ViPNet host type	String	**Client** **Coordinator** **Not defined**
Allowed traffic absence timeout when working in the dynamic address translation mode	A timeout for sending UDP packets to maintain a connection with a coordinator	Integer	**25**
IP packets log version	IP packets log version	2 numbers divided by a period	**3.0 format** **2.8 format**
Firewall address	IP address of the firewall behind which the host is placed	4 numbers divided by a period For example: **10.0.2.20**	
Firewall port	Firewall port for UDP packets	Integer	Possible values range **from 1 to 65535**
Fixed external IP address for access through the firewall is enabled	Fixed firewall settings flag	String	**Yes** **No**

Parameter name	Description	Format	Possible values
Proxy server's ID	Identifier of the ViPNet coordinator used as a proxy server	A hexadecimal number For example: **0001027d**	

Table 13: ViPNet Monitor parameters: Tunneled IP addresses ranges

Parameter name	Description	Format	Possible values
Start IP address*	Start IP address of the tunneled addresses range	4 numbers divided by a period For example: **192.168.14.251**	
End IP address*	End IP address of the tunneled addresses range	4 numbers divided by a period	

Table 14: Network interfaces: General characteristics

Parameter name	Description	Format	Possible values
Interface name	System name of the network interface	String For example: **eth0**	
List of access IP addresses	List of network interface IP addresses	A string that consists of an IP address or several IP addresses divided by a comma For example: **10.0.2.20**	

Parameter name	Description	Format	Possible values
Level of unencrypted IP packets processing	Current interface security level	Integer	Possible values range **from 1 to 5**
Level of unencrypted IP packets processing used on startup	Security level set on the host on the ViPNet Monitor startup	Integer	Possible values range **from 1 to 5**
Subnet mask	Network interface subnet mask	4 numbers divided by a period For example: **255.255.255.0**	
Interface type	A type of interface on a ViPNet host, which shows whether this interface is used to connect to a firewall	String	**External** **Internal**
Interface status	Current state of the network interface	String	**Accessible** **Unreachable**

Table 15: Network interfaces: Statistics

Parameter name	Description	Format	Possible values
Incoming			
The number of allowed non-encrypted IP packets The number of blocked non-encrypted IP packets The number of allowed encrypted IP packets	For each parameter, the number of packets is displayed (the **Number** string) and the total size of the packets (the **Total** string). The size is measured in megabytes	**Number** is an integer. **Total** is an integer.	

Parameter name	Description	Format	Possible values
The number of blocked encrypted IP packets	(**MB**) and displayed only starting with 3.1.3 version for ViPNet Client/Coordinator or with 3.6.1 version for ViPNet Coordinator Linux.		
The number of allowed broadcast IP packets			
The number of blocked broadcast IP packets			
The number of allowed encrypted broadcast IP packets			
The number of blocked encrypted broadcast IP packets			
Outgoing			
The number of allowed non-encrypted IP packets	For each parameter, the number of packets is displayed (the **Number** string) and the total size of the packets (the **Total** string). The size is measured in megabytes (**MB**) and displayed only starting with 3.1.3 version for ViPNet Client/Coordinator or with 3.6.1 version for ViPNet Coordinator Linux.	**Number** is an integer. **Total** is an integer.	
The number of blocked non-encrypted IP packets			
The number of allowed encrypted IP packets			
The number of blocked encrypted IP packets			
The number of allowed broadcast IP packets			
The number of blocked broadcast IP packets			
The number of allowed encrypted broadcast IP packets			
The number of blocked encrypted broadcast IP packets			

Parameter name	Description	Format	Possible values
Integral parameters			
Total incoming IP traffic*	Total incoming IP traffic since the last request, in megabytes (**MB**)	Integer	
Total outgoing IP traffic*	Total outgoing IP traffic since the last request, in megabytes (**MB**)	Integer	
Total*	Total incoming and outgoing IP traffic since the last request, in megabytes (**MB**)	Integer	
Load on a network interface*	Average traffic rate on the interface during the last polling period	A decimal fraction with two decimal digits	
	Measured in megabytes per second (**MB/sec**)	For example: **24.86 MB/sec**	

Table 16: Network interfaces: IP packets log settings

Parameter name	Description	Format	Possible values
Maximum IP packets log size	Measured in megabytes (**MB**)	Integer	
		For example: **1 MB**	

Parameter name	Description	Format	Possible values
Logs aggregation period	A time interval within which similar events are joined into one entry Measured in seconds (**sec**)	Integer For example: **3600 sec**	
Log all IP packets	Enable or disable logging any IP packets	String	**On** **Off**
Log broadcast IP packets	Enable or disable logging broadcast IP packets	String	**On** **Off**
For TCP connections, log only the remote server port	Enable or disable logging only the server port for TCP connections	String	**On** **Off**

Table 17: MFTP

Parameter name	Description	Format	Possible values
MFTP status*	Current MFTP status	String	**Online** **Offline** **Unknown** **Not available** **Not defined**

Parameter name	Description	Format	Possible values
The number of envelopes in the queue*		Integer	
Total size of all the envelopes in the queue*	Measured in megabytes (**MB**)	Integer	

Table 18: Passive cluster node parameters

Parameter name	Description	Format	Possible values
Host status	The status of the passive cluster node	String	**Accessible** **Unreachable** **Not defined**
ViPNet MFTP status*	The status of the MFTP component on the passive cluster node	String	**Online** **Offline** **Unknown** **Not available** **Not defined**
Iplir daemon status*	The status of the iplir daemon on the passive cluster node	String	**Online** **Offline** **Unknown** **Not available** **Not defined**

Parameter name	Description	Format	Possible values
Failover module status*	The status of the Failover component on the passive cluster node	String	**Online** **Offline** **Unknown** **Not available** **Not defined**
CPU load*	CPU load percentage (%)	Integer	
Total physical memory (RAM)*	Measured in megabytes (**MB**)	Integer	
Free physical memory (RAM)*	Measured in megabytes (**MB**)	Integer	

Parameters Monitored on Public Hosts

In this appendix, you will find a list of parameters that are monitored in the current version of the ViPNet StateWatcher monitoring system. The parameters are joined into the same logical groups as in Monitoring Web Access. Each logical group of parameters is described in a separate table. For each parameter, you can see its name, format, brief description, type of data, and, if necessary, the possible values.

Table 19: System parameters

Parameter name	Description	Format	Possible values
Host description	SNMP host description	String	
Up time	The time of uninterrupted operation of a host	HH:MM:SS.CS (centiseconds) For example: **11:43:23.33**	
Contact information	Contact information for the person who administers this public host	String	
Host name	The SNMP host's name.	String	
Location	SNMP host location	String	
Amount of RAM	RAM size (in KB)	KB	
Host's current time	The current time and date on the monitored host	HH:MM:SS - DD.MM.YYYY For example: **10:54:27 - 02.02.2013**	

Table 20: Network settings

Parameter name	Description	Format	Possible values
Router	Whether the host is a router (performs forwarding) or not	Integer	
TTL	The lifespan of an IP datagram (TTL)	Integer	
The number of received IP datagrams		Integer	
The number of incoming IP datagrams containing errors in the packet heading		Integer	
The number of IP datagrams discarded because of an incorrect IP address		Integer	
Number of IP datagrams that were being attempted to be forwarded		Integer	
The number of IP datagrams whose protocol code is not supported		Integer	
The number of IP datagrams discarded because the buffer is full		Integer	
The number of incoming IP datagrams successfully processed on the IP layer		Integer	

Parameter name	Description	Format	Possible values
The number of IP and ICMP datagrams intended for sending		Integer	
The number of IP and ICMP datagrams intended for sending, but discarded because the buffer is full		Integer	
The number of routing errors		Integer	
Maximal timeout in seconds for the fragments assembling		Integer	
The number of received fragments	The number of received IP datagram fragments	Integer	
The number of received and successfully assembled IP datagrams		Integer	
The number of IP datagrams that could not be assembled	The number of IP datagrams that could not be assembled for some reasons	Integer	
The number of successfully fragmented IP datagrams		Integer	
The number of IP datagrams intended for fragmenting, but whose fragmenting is impossible (for example, because of a flag)		Integer	

Parameter name	Description	Format	Possible values
The number of IP datagram fragments created by this host	The number of IP datagram fragments created by this SNMP host	Integer	

Table 21: Network interfaces

Parameter name	Description	Format	Possible values
Number of interfaces	The number of network interfaces	Integer	
Text description of the interface		String	
Interface type		Integer For example: **6** — Ethernet **9** — 802.5 Token Ring **23** — PPP **28** — SLIP	
Maximum Transmission Unit (MTU)	The largest data unit that can be transmitted (maximum transmission unit)	Integer	
Speed	The interface speed in bps	bps	

Parameter name	Description	Format	Possible values
Physical address		Physical address For example, **a0:b3:cc:a0:ac:26**	
The required state of the interface		Integer	Possible values: **1** — the interface is enabled **2** — the interface is disabled **3** — the interface is being checked
Current state of the network interface		Integer	Possible values: **1** — the interface is enabled **2** — the interface is disabled **3** — the interface is being checked
Current state time	The time when the interface assumed the current state	HH:MM:SS.CS (centiseconds) For example: **11:43:23.33**	
The number of received bytes		Byte	
The number of ordinary packets delivered to the top system level	The number of unicast packets delivered to the top system level	Integer	
The number of broadcast and multicast packets delivered to the top system level	Received broadcast and multicast IP packets delivered to the top system level	Integer	

Parameter name	Description	Format	Possible values
The number of received but discarded packets		Integer	
The number of packets received with errors		Integer	
The number of packets whose protocol code contains errors		Integer	
The number of sent bytes		Integer	
The number of ordinary packets received from the top system level	The number of unicast packets received from the top system level	Integer	
The number of broadcast and multicast packets received from the top system level	The number of broadcast and multicast packets received from the top system level	Integer	
The number of sent but discarded packets		Integer	
The number of sent packets containing errors		Integer	
The number of IP packets in the send queue		Integer	

Table 22: Address information table (ARP)

Parameter name	Description	Data type	Possible values

Parameter name	Description	Data type	Possible values
Low bit value	The low bit value for a broadcast address	Integer	Possible values are **0** and **1** (usually **1**)
Identifier	Interface identifier	Integer	
IP address	IP address of the interface	IP address For example, **110.33.7.83**	
Subnet mask	Subnet mask for this interface	IP address For example, **255.255.255.0**	
IP datagram size	The maximum size of the IP datagram that can be collected	Integer	Possible values range from **0** to **65535**

Table 23: Data storages

Parameter name	Description	Data type	Possible values
Data block size (bytes)	The data block size in bytes	Byte	
Storage index	Data storage index	Integer	
Allocation units size		Integer	
Description	Data storage description	String	
Used allocation units amount		Integer	

Parameter name	Description	Data type	Possible values
The number of requests to the data storage	The number of requests to the data storage that could not be processed because of a lack of space in the storage	Integer	
Storage type	Data storage type	String (containing the data storage identifier)	

Table 24: Disk data storages

Parameter name	Description	Data type	Possible values
Ejectable	The disk storage can be ejected	Boolean	Possible values — **true** and **false**
Size	The size of the disk storage	KB	
Disk type	The type of a disk storage	Integer	Possible values: **8** — RAM **7** — optical RW **6** — optical WORM **5** — optical ROM **4** — floppy **3** — hard drive

Parameter name	Description	Data type	Possible values
			2 — unknown
			1 — other
Access	Permissions for accessing the device	Integer	Possible values:
			1 — read and write
			2 — read only

Table 25: Running processes

Parameter name	Description	Data type	Possible values
Process identifier	Process ID in the system	Integer	
Parameters	A description of the parameters supplied to CPU when it was initially loaded	String	
Process status	The status of the running process	Integer	Possible values:
			1 — launched
			2 — operable
			3 — inoperable
			4 — error
Process location	Location on a disk where the process was launched	String	

Parameter name	Description	Data type	Possible values
Process type		Integer	Possible values: **1** — unknown **2** — operating system **3** — driver **4** — application process
Process ProductID	Application identifier for the running process	String	
Process description	Description of the running process	String	

Table 26: Installed applications

Parameter name	Description	Data type	Possible values
Application type	The type of the installed program	Integer	Possible values: **1** — unknown **2** — operating system **3** — driver **4** — program
Application index	The index of the installed program	Integer	

Parameter name	Description	Data type	Possible values
Application description	A description of the installed program	String	
Program ID		String	
Modified	The date and time when the application was last modified	HH:MM:SS - DD.MM.YYYY For example: **10:54:27 - 02.02.2013**	

Note: The SNMP client running on a host may fail to provide the monitoring server with a full list of applications installed on this host. Thus, some applications may be missing.

Table 27: Network services

Parameter name	Description	Data type	Possible values
Number of network services		Integer	
Pause	The ability to pause the service	Integer	Possible values: **1** — pause impossible **2** — pause possible
Installation status	The status of the service installation	Integer	Possible values: **1** — not installed

Parameter name	Description	Data type	Possible values
			2 — pending installation **3** — pending deletion **4** — installed
Current state	Current state of the service	Integer	Possible values: **1** — active **2** — continue pending **3** — pause pending **4** — pause
Service name		String	
Uninstallation	The ability to delete the service	Integer	Possible values: **1** — can't be deleted **2** — can be deleted

Table 28: Printer parameters

Parameter name	Description	Data type	Possible values
Printer name		String	
Serial number	Serial number of the printer	String	

Parameter name	Description	Data type	Possible values
The number of critical events		Integer	
The number of all events		Integer	

ViPNet IDS Monitoring Parameters

In this appendix, you will find a list of ViPNet IDS software and hardware appliance parameters that are monitored in the current version of the ViPNet StateWatcher monitoring system. The parameters are logically grouped the same way as in the monitoring web access interface. Each logical group of parameters is described in a separate table. For each parameter, you can see its name, format, brief description, type of data, and, if necessary, the possible values.

Table 29: System options

Parameter name	Description	Format	Possible values
Host description	Public host description	String	
Up time	The time of uninterrupted operation of a host	HH:MM:SS.CS (centiseconds) For example: **11:43:23.33**	
Contact information of the person who administers this host	Contacts of the ViPNet IDS administrator	String	
Host name	The public host's name	String	
Location	Public host's location	String	
Current sensor identifier	ViPNet IDS sensor's ID	Integer	

Parameter name	Description	Format	Possible values
Report started	Start of the time period, during which the monitoring server was collecting data from the ViPNet IDS appliance	HH:MM:SS - DD.MM.YYYY For example: **10:54:27 - 02.02.2013**	
Report ended	End of the time period, during which the monitoring server was collecting data from the ViPNet IDS appliance	HH:MM:SS - DD.MM.YYYY For example: **10:54:27 - 02.02.2013**	
Total number of attacks registered on the current sensor	The number of network attacks this sensor has detected	Integer	

Table 30: Available sensors

Parameter name	Description	Format	Possible values
Sensor identifier	ViPNet IDS sensor's ID	Integer	
Sensor name	ViPNet IDS sensor's name	String	

Table 31: Attacks statistics

Parameter name	Description	Format	Possible values
Sensor identifier	ViPNet IDS sensor's ID	Integer	

Parameter name	Description	Format	Possible values
Attack severity	Attack's severity level: Critical, Warning, or Standard	Integer	Possible values: **Critical** means a high severity level **Warning** means a middle severity level **Standard** means a low severity level
Attacks number	The number of attacks with the specified severity level	Integer	

Table 32: Attacks list

Parameter name	Description	Format	Possible values
Sensor's ID	ViPNet IDS sensor's ID	Integer	
Attack's ID	Network attack's ID	Integer	
Attack's name	Network attack's name	String	
Attack's severity level	Attack's severity level: Critical, Warning, or Standard	Integer	Possible values: **Critical** means a high severity level **Warning** means a middle severity level

Parameter name	Description	Format	Possible values
			Standard means a low severity level
Number of attacks	The number of attacks with the specified ID	Integer	
Attack URL	A URL address with a description of the attack	URL	

Table 33: Hosts under attack

Parameter name	Description	Format	Possible values
Sensor identifier	ViPNet IDS sensor's ID	Integer	
ViPNet host identifier	Attacked host's identifier	Integer	
Host IP address	Attacked host's IP address	IP address	
Number of attacks targeting this host	The number of network attacks to this host	Integer	

Table 34: Attacking host list

Parameter name	Description	Format	Possible values
Sensor identifier	ViPNet IDS sensor's ID	Integer	

Parameter name	Description	Format	Possible values
ViPNet host identifier	Attacker host's ID	Integer	
Host IP address	Attacker host's IP address	IP address	
Number of attacks initiated by this host	The number of network attacks from this host	Integer	

Glossary

A

Authentication

The process of identifying an individual usually based on a user name and a password. In security systems, authentication is distinct from authorization, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

C

Cascade

A multilevel hierarchical structure of child-parent connections between monitoring servers. In a cascade, every child monitoring server transfers the hosts' monitoring data to its parent monitoring server. The cascade interaction structure balances the monitoring load between monitoring servers and allows you to monitor a segmented network even when ViPNet hosts in its segments are not linked with the parent monitoring server.

Cascaded monitored host

A host that is monitored by a given monitoring server not directly, but through its direct child server or through a chain of its child monitored servers. The given monitoring server only

receives notifications about events on the cascaded monitored host from its child monitoring servers.

Customization pack

A pack of settings for configuring the monitoring system according to your needs. A customization pack may contain localization files, additional built-in processing rules, email templates, and customized icons for host types in your company. By default, a customization pack is installed when you install the Monitoring Server software on a new computer or when you upgrade your Monitoring Server program. You may update the installed customization pack with a `StateWatcherInstaller.jar` file.

D

Data rotation

A procedure for deleting outdated information, such as:

- unprocessed host parameters;
- monitoring events registered as a result of processing host parameters with rules.

The monitoring server administrator may change rotation parameters in advanced settings of Monitoring Server.

E

Email notification templates

Files with a `.jasper` extension, which are compiled templates of Jasper reports. To work with these templates, you may use a freely distributed report designer iReport that is included in the distribution kit. To download the latest iReport version, click this link http://jasperforge.org/projects/ireport/.

M

Monitored group

A named subset from the total set of hosts monitored by the monitoring server. Groups are user-defined logical units of monitored hosts united on the basis of belonging to the same department, geographic location, and so on. On a monitoring server, you can specify monitored groups regardless of groups specified on the other monitoring servers. Some monitored groups are built-in: they are present on all monitoring servers for service needs and can't be discarded.

Monitored host

A ViPNet host (a client or a coordinator) that is subject to monitoring in ViPNet StateWatcher monitoring system. Every monitoring server has its own list of monitored hosts. A host may be monitored by more than one monitoring server.

Monitoring event

Any alteration of the state of a host, traced by processing rules, which has been detected on a monitored host. Every monitoring event is attributed a severity level, which reflects the importance of the event for the host's operation. Every monitoring event is followed by a notification. You may set the notification type in a corresponding processing rule.

Monitoring server

A ViPNet host (client) with special software installed that monitors the network. A monitoring server performs all the main functions for network monitoring: collecting, processing, and storing the hosts' state data, notifying its users about host operation failures and critical events. The ViPNet StateWatcher monitoring system may include more than one monitoring server.

Monitoring Web Access

A web interface, via which you can access the monitoring server for its configuring, accessing its monitoring database and receiving notifications. Access is performed through a web browser. The same monitoring client may be used to access more than one monitoring server.

N

Notifications

Informational messages, which are created as a result of events detected when executing a processing rule. The notifications can be of the following types:

- in the host list;
- pop-up messages;
- sound;
- by email;
- by Business Mail;
- by SMS.

P

Processing rule

A rule that determines processing of monitored hosts' parameters and registers the monitoring events. A range of rules is built into a customization pack. By default, these rules are present on all monitoring servers that have the default customization pack installed. You may create additional processing rules on any monitoring server.

Protected host

A host with installed ViPNet software that can encrypt traffic in the network layer.

R

Raw database

A database temporarily storing monitored host parameters, before they are processed according to the processing rules. The raw database is organized as an OLTP (Online Transaction Processing) base.

Role

A ViPNet host's functionality, designed to solve user-oriented and service tasks for a ViPNet network. Roles are used in network licensing (by being specified in the license file) and define which program features can be used and which software can be installed on your ViPNet host.

Roles may have some attributes: user permissions that affect the choice of features and quantitative characteristics.

Roles for each ViPNet host are specified by the ViPNet network administrator in ViPNet Network Manager.

T

Tunneled host

A host where no ViPNet software encrypting traffic on the network layer is installed. In a potentially dangerous network section, the traffic of this host is encrypted and then decrypted on the coordinator it is placed behind.

U

Unprocessed parameters

Monitored hosts' parameters that have been collected and stored by the monitoring server but have not yet been processed with the processing rules.

Unprotected host

A host that exchanges unencrypted traffic with a ViPNet host.

V

ViPNet Business Mail

A program, which allows you to exchange protected emails between ViPNet hosts. With ViPNet Business Mail, ViPNet users linked with each other can exchange protected email messages.

ViPNet Business Mail is part of the ViPNet Client software. You can install it together with other components of this software or alone.

ViPNet Business Mails has standard email client features, such as:

- Email sending and receiving.
- Email attachments sending and receiving.
- Digitally signing email messages and their attachments.
- Encrypting email attachments.

See also: ViPNet network (on page 125).

ViPNet network

A logical network that is created and maintained with ViPNet software and consists of ViPNet hosts.

A ViPNet network has a special addressing system, which provides for data exchange between its hosts. Each ViPNet network has its own unique number (host ID).

ViPNet Network Control Center

In a network managed using the ViPNet Administrator software, ViPNet Network Control Center is a program that is a part of ViPNet Administrator. It is designed to create and configure ViPNet networks. Its main features are as follows:

- Creating a virtual network (creating network objects and their links, including partner network links);
- Changing network configuration;
- Generating and distributing protected host links;
- Distributing host keys and user keys;
- Generating information on users' links for ViPNet Key and Certification Authority;
- Granting permissions to ViPNet users.

In a network managed using the ViPNet Network Manager software, ViPNet Network Control Center is the ViPNet network administrator's workstation. In Network Control Center, the administrator creates a ViPNet network structure, creates and distributes key set and ViPNet software updates.

ViPNet StateWatcher monitoring system

The ViPNet StateWatcher monitoring system is designed for checking the network status of ViPNet hosts, for monitoring security events on the hosts, for detecting malfunctioning in hosts' operation, and for notifying hosts' users promptly about any network issues.

Index

C
Configuring a Current Settings Tile • 39
Configuring a Graph Tile • 39
Configuring Pop-up Notifications • 61
Customization pack • 44

D
Data rotation • 33

E
Exporting the Monitoring Events History • 53

M
Monitored host • 6
Monitoring event • 59
Monitoring Hosts on a Dashboard • 12
Monitoring Hosts on a Map • 63
Monitoring the Network Health • 40

P
Parameters Monitored on Hosts • 33
Pop-up Messages • 34

R
Recentering the Map and Positioning on the Map • 46
Recommended Internet Explorer Configuration • 11

S
Searching for Geographical Objects • 46, 47
Searching for Hosts on the Map • 46, 47
Structure of the Events History Export File • 55
Structure of the Unprocessed Host Parameters Export File • 58

V
Viewing Information about a Monitored Host • 13, 46, 49, 63
ViPNet Business Mail • 65
ViPNet network • 125
Visual notification on the Map • 46